1/2013

Datenschutz Nachrichten

36. Jahrgang
ISSN 0137-7767
9,00 Euro



■ Löschen nach Regeln ■ Erfahrungen bei der Umsetzung eines Löschkonzeptes ■ Vertrauliche Papierunterlagen vernichten ■ Datenlöschung in SAP - Wo liegt das Problem? ■ Meldegesetz: Vermittlungsausschuss kippt Widerspruchslösung ■ Wann ist ein Nein ein Nein? ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechung ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine

Freitag, 12. April 2013, 18:00 Uhr
Verleihung der BigBrotherAwards 2013
Bielefeld
http://www.bigbrotherawards.de

Samstag, 13. April 2013
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Mittwoch, 1. Mai 2013
Redaktionsschluss DANA 2/13
Thema „Konzernprivileg“.

Montag, 13. Mai 2013 bis
Donnerstag, 16. Mai 2013
14. Datenschutz-Kongress 2013
Berlin
http://www.datenschutzkongress.de/

Montag, 17. Juni 2013 und Dienstag, 18. Juni 2013
DuD 2013 – 15. Jahresfachkonferenz
Datenschutz und Datensicherheit
Berlin.
http://www.computas.de/konferenzen/dud_2013/DuD_2013.html
Siehe auch Hinweis auf Seite 37

Sonntag, 28. Juli 2013, 10:00 Uhr
DVD-Vorstandssitzung
Berlin. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Mittwoch, 11. September 2013 bis
Samstag, 14. September 2013
14. Herbstakademie 2013
Law as a Service (LaaS) – Recht im Internet- und Cloud-Zeitalter
Humboldt Universität in Berlin
http://www.dsri.de/herbstakademie/herbstakademie.html

Montag, 16. September 2013 bis
Freitag, 20. September 2013
GI-Jahrestagung 2013
Koblenz
http://www.informatik2013.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
36. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
Konto 1900 2187, BLZ 370 501 98,
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Karin Schuler
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen
Fotos
Frans Jozef Valenta

Editorial

Liebe Leserinnen und Leser,

vermutlich haben die meisten von uns eine gewisse Neigung, Dinge des Lebens länger aufzubewahren, als sie tatsächlich gebraucht werden. Seien es die alten Kontoauszüge aus der Studentenzeit, die Liebesbriefe des Verflossenen oder die vergilbten Kinderbilder. Das Festhalten an Erinnerungen ist menschlich und im Privaten meist unspektakulär. Doch der hier harmlose Jäger- und-Sammler-Trieb gefährdet im Unternehmensumfeld das informationelle Selbstbestimmungsrecht unzähliger Betroffener. Schaut man manche Datenspeicher von Unternehmen an, so fühlt man sich an zwanghaftes Horten erinnert. Da finden sich Kaffeekassenlisten der letzten zehn Jahre neben eingescannten Arbeitsunfähigkeitsbescheinigungen und Kommt/Geht-Zeiten der letzten zwanzig Jahre. Denn Speicher ist preiswert und dessen Erweiterung allemal bequemer, als sich über die systematische und rechtskonforme Löschung Gedanken zu machen.
Leider ist dieses Verhalten so kurzsichtig wie rechtswidrig. Wie es stattdessen ablaufen sollte, berichtet Volker Hammer in seinem Beitrag über eine Leitlinie zur Erstellung von Löschkonzepten. Diese ist wesentlich auf Erfahrungen gegründet, die bei Toll Collect mit der systematischen Entwicklung von Löschverfahren gesammelt wurden – ein Erfahrungsbericht von Reinhard Fraenkel und Volker Hammer verdeutlicht den Praxisbezug. Hans-Hermann Schild befasst sich mit der Chronik einer langen Leidensgeschichte: der Möglichkeit geregelter Datenlöschung in SAP und Hajo Köppen informiert über die Änderungen anlässlich einer neuen DIN zur Vernichtung von Datenträgern.
Mit diesen Beiträgen zum Schwerpunktthema und den üblichen Datenschutznachrichten aus Deutschland und aller Welt wünsche ich Ihnen eine erkenntnisreiche Lektüre.

Karin Schuler

Autorinnen und Autoren dieser Ausgabe:

Reinhard Fraenkel
Nach verschiedenen Tätigkeiten in der Industrie seit 1994 als Rechtsanwalt in Gütersloh tätig. Zu seinen Arbeitsschwerpunkten zählt das Datenschutzrecht. Seit August 2004 ist er externer Datenschutzbeauftragter der Toll Collect GmbH.
post@kanzlei-fraenkel.de

Dr. Volker Hammer
Consultant bei Secorvo Security Consulting. Seit Mitte 2003 unterstützt er die Toll Collect GmbH in verschiedenen Datenschutz-Projekten. Er war Leiter des DIN/INS-Projekts, in dem die hier beschriebene Leitlinie entstand.
volker.hammer@secorvo.de

Hajo Köppen
Assessor. jur., Referent für hochschulpolitische Fragen, Datenschutzbeauftragter und Dozent für Datenschutzrecht an der Technischen Hochschule Mittelhessen,
hajo.koeppen@verw.thm.de, www.thm.de/datenschutz, www.zaftda.de

Hans-Hermann Schild
Vorsitzender Richter am Verwaltungsgericht Wiesbaden.1997 war er als Referatsleiter zum Bundesbeauftragten für den Datenschutz abgeordnet, um an der Umsetzung der EG-Datenschutzrichtlinie beratend mitzuwirken. Autor von vielen Fachpublikationen zum Datenschutzrecht.
HH.Schild@t-online.de

Karin Schuler
Beraterin für Datenschutz und IT-Sicherheit.
Vorsitzende der Deutschen Vereinigung für Datenschutz e.V.
schuler@datenschutzverein.de

Volker Hammer

Löschen nach Regeln

Standardisierungsmöglichkeiten für ein Löschkonzept

1 Motivation

In sehr vielen Geschäftsprozessen und IT-Anwendungen werden personenbezogene Daten verwendet. Diskutiert man mit Anwendern oder Entscheidungsträgern über das Löschen derartiger Daten, so scheinen die Hürden unüberwindlich. So wird beispielsweise vorgebracht: Technisch sei es ungeheuer schwierig oder eine Löschung gar nicht vorgesehen. Oder: Es gäbe niemanden, der entscheiden könne, dass Prozesse abgeschlossen sind und nicht doch noch eine Nachfrage oder Prüfung durch Finanzamt oder Wirtschaftsprüfer erfolgt. Und immer wieder: Man wisse ja auch nicht, ob die Daten nicht doch für eine – noch neu zu entwickelnde – statistische Auswertung, Marketingmaßnahme oder andere Idee benötigt würden.

Viele Anwender wollen Daten schlichtweg nicht löschen. Die personenbezogenen Daten unterliegen aber dem Datenschutzrecht, das auch Löschvorgaben enthält: Sie dienen dem Schutz der Betroffenen, denn nach dem Löschen ist eine unzulässige oder unerwünschte Verwendung der Daten nicht mehr möglich. Die §§ 20 Abs. 2 Nr. 2 und 35 Abs. 2 Nr. 3 BDSG fordern die Löschung personenbezogener Daten, wenn ihre Verarbeitung nicht mehr erforderlich ist. Damit wird § 4e BDSG konkretisiert, denn § 4e Nr. 7 BDSG statuiert die Pflicht der verantwortlichen Stelle, Regelfristen für die Löschung personenbezogener Daten festzulegen. Spezialgesetze können außerdem für bestimmte Datenarten hinsichtlich der Löschung engere Vorgaben als das BDSG treffen.

In der Fachöffentlichkeit ist man sich weitgehend einig, dass bezüglich des Löschens ein großes Vollzugsdefizit besteht – allerdings begleitet von einer gewissen Hilflosigkeit. Die Toll Collect GmbH[1] zeigt jedoch, wie es gehen kann: Sie realisierte schon zum Mautstart ein Löschkonzept für die Mautdaten. Dieses Konzept wurde in den vergangenen Jahren überaus erfolgreich auch für alle anderen Datenbestände mit Personenbezug weiterentwickelt und umgesetzt. Wichtige Elemente der Vorgehensweise wurden schon 2007 veröffentlicht.[2] Aus Kontakten mit dem Deutsches Institut für Normung e. V. (DIN) ergab sich schließlich die Frage, ob die verfolgte Vorgehensweise nicht auf andere Organisationen übertragbar sei. Im Rahmen des Programms „Innovation mit Normen und Standards – INS“ wurde daher ein Projekt durchgeführt (kurz *DIN/INS-Projekt*), um die Standardisierbarkeit des Ansatzes zu prüfen.[3]

2 Unterstützung für das Löschen personenbezogener Daten?

Die oben beschriebenen Bedenken werden selbstverständlich nicht nur aus Bequemlichkeit vorgebracht oder weil interne Blockaden überwunden werden müssen. Auch objektiv verlangt die rechtskonforme Umsetzung der Löschgebote eine höchst komplexe Subsumption für die Bestimmung der Fristen, die den Wegfall der Erforderlichkeit für die Speicherung festlegen. Das sichere und systematische Löschen personenbezogener Daten ist für eine verantwortliche Stelle schwierig, denn:

- für die Fristbestimmung müssen unbestimmte Rechtsbegriffe ausgelegt werden,
- das Ende von Prozessen, in denen die Daten benötigt werden, muss identifiziert werden, um konkrete Löschzeitpunkte festlegen zu können, und
- die Löschmechanismen müssen in den betroffenen IT-Systemen und Prozessen implementiert werden.

Allgemeine und unspezifische Aufforderungen zum Löschen werden in einer verantwortlichen Stelle kaum erfolgreich sein – sie führen allenfalls zufällig und in Einzelfällen zum Erfolg. Angesichts der Komplexität kann die Aufgabe wohl nur nach systematischer Analyse und mit Hilfe klar strukturierter Regeln gelöst werden.

Welche Hilfestellungen sind möglich?

Können die Löschregeln zwischen Organisationen übertragen werden? Im Allgemeinen wohl kaum. Denn das Prinzip der „Erforderlichkeit“ des BDSG stellt auf die zulässigen Verwendungszwecke der verantwortlichen Stelle ab – und die sind so verschieden wie es Unternehmen und Behörden sind. Geschäftsprozesse, Verträge mit Kunden oder Arbeitnehmern, gesetzliche Pflichten oder Aufgaben, die Größe der Organisation oder ihre Technikausstattung unterscheiden sich. All diese Faktoren haben Einfluss auf den richtigen Zeitpunkt der Löschung und auf die daraus resultierenden Löschregeln. Allgemeine, direkt übertragbare Regeln wird es daher nur in gleich gelagerten Anwendungsfeldern wie beispielsweise der Personalverwaltung geben können.

Im DIN/INS-Projekt zum Löschkonzept war daher zu untersuchen, nach welchem Schema eine Organisation ihr Löschkonzept entwickeln kann und welche Aspekte des Löschens von personenbezogenen Daten dabei zwischen Organisationen übertragen werden können. Für diese Aspekte war zu prüfen, ob Hilfestellungen gegeben werden können, um die rechtlichen Pflichten in Organisationen umzusetzen.

Ziel: organisationsspezifisches Löschkonzept

Organisationsweites Löschen muss als eine kontinuierliche Aufgabe verstanden werden. Geschäftsprozesse und die IT-Landschaft sind heute so dyna-

misch, dass die Löschregeln und die Verantwortlichkeiten für die Umsetzung immer wieder zu überprüfen, zu ergänzen und anzupassen sind. Um eine rechtskonforme, geordnete Löschung von personenbezogenen Daten sicherzustellen, müssen verantwortliche Stellen ein Regelwerk entwickeln und Verantwortung für die Aufgaben der Löschung zuweisen. Dieses Regelwerk wird als Löschkonzept bezeichnet.

Zwar müssen konkrete Löschregeln aus den spezifischen Gegebenheiten in der Organisation abgeleitet werden; die Vorgehensweise, um sie festzulegen, ist aber übertragbar. Bei der Toll Collect konnten in den vergangenen Jahren hierzu zentrale Erkenntnisse gewonnen werden. Diese sollten im Rahmen des Projekts mit andern Vertretern der Fachöffentlichkeit diskutiert und verallgemeinert werden.

Mit übertragbaren Hilfestellungen, so die Erwartung, verbessern sich in jeder Organisation die Erfolgsaussichten für die Entwicklung eines konkreten Löschkonzepts wesentlich. Wenn die verantwortliche Stelle auf eine bewährte Vorgehensweise zurückgreifen kann, kann sie Fehlversuche vermeiden.

Die „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“[4], im Weiteren kurz: *Leitlinie*, gibt Hilfestellungen für die Kernaufgaben in Löschprojekten. Mit ihrer Hilfe kann ein Löschkonzept effizient erstellt werden. Die Leitlinie ist das Ergebnis des DIN/INS-Projekts, das von intensiven Diskussionen mit Datenschützern aus Industrie und Aufsichtsbehörden begleitet wurde.[5]

3 Die Leitlinie Löschkonzept

In einem Löschkonzept legt eine verantwortliche Stelle fest, wie sie die datenschutzrechtlichen Pflichten zur Löschung von personenbezogenen Daten erfüllen will. Die Leitlinie beschreibt, wie ein solches Löschkonzept etabliert werden kann. Dazu gehören:

- Vorgehensweisen, durch die Löschregeln für personenbezogene Datenbestände festgelegt werden,
- eine Übersicht über notwendige Umsetzungsvorgaben zur Löschung innerhalb der verantwortlichen Stelle,
- Vorschläge für die Dokumentationsstruktur, Anforderungen an Prozesse und Verantwortung für die Etablierung, Fortschreibung und Umsetzung des Löschkonzepts.

3.1 Löschregeln festlegen

Ein Löschkonzept kann nur dann mit akzeptablem Aufwand etabliert werden, wenn alle Beteiligten die Löschregeln nachvollziehen können und die Komplexität der Umsetzung überschaubar bleibt. Einfache Regeln sind daher der Schlüssel zum Erfolg.

Kern eines Löschkonzepts ist es, die Löschregeln festzulegen. Eine Löschregel enthält eine Löschfrist und eine Bedingung für den Startzeitpunkt des Fristlaufs. Die Löschregeln werden jeweils für Datenarten bestimmt. In den Datenarten werden einzelne Bestände von personenbezogenen Daten, die in der verantwortlichen Stelle für die gleichen Zwecke verwendet werden, zusammengefasst.[6] Beispielsweise könnten bei einem Telekommunikations-Provider als Datenarten Stammdaten, Standortdaten, Verkehrsdaten, Abrechnungsdaten und Einzelverbindungsnachweise unterschieden werden. Die Bestände einer Datenart werden hinsichtlich der Löschung gleich behandelt.

Datenarten sind meist einfach zu bestimmen. Die genaue Festlegung der „Erforderlichkeit“ als Voraussetzung für eine Löschfrist ist dagegen oft mit sehr großem Aufwand verbunden. Da die Etablierung eines Löschkonzepts an diesem Aufwand scheitern kann,[7] sind besonders hierfür geeignete Ansätze gefordert. Die Leitlinie schlägt dazu die folgenden Vorgehensweisen vor:

- Verwendung von **Standardfristen**. Eine zu differenzierte Landschaft von Löschfristen ist für die Beteiligten in einer Organisation nicht handhabbar. Die Leitlinie geht deshalb von der Annahme aus, dass ein rechtlich vertretbarer Kompromiss zwischen den Löschvorgaben der Rechtsnormen und der Praktikabilität von Löschprozessen gefunden werden muss.[8]
- **Varianten für die Analyse von Löschfristen**. Die Leitlinie geht davon aus, dass Rechtsvorschriften unterschiedlich große Gestaltungsspielräume einräumen, um Löschfristen zu bestimmen: Für wenige Datenbestände kann die Frist aus den Rechtsvorgaben entnommen werden. Spezifische Rechtsvorschriften ohne konkrete Fristvorgabe oder Datenbestände mit hoher Sensitivität erfordern eine enge Fristregelung und daher eine genaue und gegebenenfalls aufwändige Analyse. Ist dagegen nur allgemein die Erforderlichkeit zu beachten, können in vielen Fällen Standardlöschfristen anhand einfacher Kriterien abgeleitet werden. Durch die Varianten können die Aufwände zur Fristanalyse wesentlich verringert werden.
- **Löschklassen** für die Zuordnung von Löschregeln zu Datenarten. Aus den Standardfristen und drei Typen von Startzeitpunkten[9] ergeben sich sogenannte Löschklassen. Die Erfahrungen zeigen, dass die Zuordnung von Löschregeln mit Hilfe der Löschklassen sehr effizient möglich ist und eine übersichtliche Struktur von Datenarten und Löschregeln ergibt.

Es bietet sich an, die Löschklassen in einer Matrix darzustellen. In der Praxis zeigt sich, dass ggf. nicht alle möglichen Kombinationen von Standardfristen und Startzeitpunkten als Löschklassen benötigt werden (siehe Abb. 1). Dadurch wird das Löschkonzept der verantwortlichen Stelle weiter vereinfacht.

Die Leitlinie gibt außerdem eine Reihe von Hinweisen, wie „Nebenbestände“ von Daten behandelt werden können. Beispiele sind die Löschung von Kopien für die Datensicherung, das Löschen in Archiven, Datenabzüge außerhalb von Regelprozessen oder das Vorhalten von Datenbeständen mit Fehlern.

3.2 Vorgaben für die Umsetzung von Löschregeln

Sind die Löschregeln festgelegt, gilt es, sie umzusetzen. Dies soll durch konkrete Umsetzungsvorgaben erfolgen. Sie richten sich an die Mitarbeiter, die für die Datenbestände verantwortlich sind. Nach der Leitlinie können folgende Umsetzungsvorgaben unterschieden werden:

- Umsetzungsvorgaben für Querschnittsbereiche; dazu gehören beispielsweise

Beispiel für eine Matrix mit Löschklassen (Toll Collect)

Startzeitpunkte	Standardfristen						
	Sofort	42 Tage	120 Tage	1 Jahr	4 Jahre	7 Jahre	12 Jahre
Ab Erhebung			Mautdaten	Mautdaten mit bes. Analysebedarf			
Ab Ende Vorgang	nmF, Web-Logs	Kurzzeit-Doku., Betriebs-Logs	EFN, voll erstattete Reklamationen	Vorgänge ohne Dokupflicht	Rekla- und Forderungsdaten	Handelsbriefe	Buchhaltungsdaten
Ab Ende Beziehung				ergänzende Stammdaten		Verträge	Kernstammdaten

Beispiel: Löschklassen bei Toll Collect

Legende:
Hellgrau unterlegt: Frist abgeleitet aus allgemeinen Gesetzen
Dunkelgrau unterlegt: Frist abgeleitet aus dem Bundesfernstraßenmautgesetz
Mittelgrau unterlegt: Frist frei gewählt

Abkürzungen: nmF = Mautdaten nicht-mautpflichtiger Fahrzeuge; EFN = Einzelfahrtennachweis

In den Zellen der Matrix sind beispielhaft Datenarten aus dem Kontext des Mautsystems angegeben. Für andere verantwortliche Stellen ergeben sich möglicherweise andere – ggf. auch zusätzliche – Standardfristen und andere Datenarten.[10]

die Maßnahmen zur Behandlung von Protokollen oder Sicherungskopien.
- Umsetzungsvorgaben für einzelne IT-Systeme; diese sind für IT-Systeme festzulegen und zu implementieren, in denen die eigentliche Datenhaltung erfolgt.
- Einzelmaßnahmen zur Löschung von Datenbeständen. Darunter fallen u. a. Anweisungen zum Löschen im allgemeinen Bürobetrieb, Arbeitsanleitungen für die Löschung von Datenbeständen in manuellen Prozessen und die Steuerung der Löschung für einzelne Datenabzüge außerhalb der Regelprozesse.
- Umsetzungsvorgaben für Auftragnehmer; diese müssen durch Verträge und Weisungen geregelt werden.

3.3 Verantwortung, Prozesse und Dokumentationsstruktur

Um ein Löschkonzept erfolgreich und dauerhaft zu etablieren, sind weitere Elemente notwendig, die ebenfalls in der Leitlinie beschrieben werden. Zunächst sind für die Aufgaben im Löschkonzept die Verantwortlichen festzulegen, z. B. in der folgenden Weise:
- **Betrieblicher Datenschutzbeauftragter** (bDSB): Pflege der Dokumente Löschkonzept, Regellöschfristen und Umsetzungsvorgaben für Querschnittsbereiche, sowie Datenschutz-Audits zum Löschen.
- **Für Datenbestände verantwortliche Mitarbeiter**: Umsetzungsvorgaben mit dem bDSB abstimmen und betrieblich überwachen.
- **IT-Entwicklung**: Löschanforderungen durchgängig in allen relevanten Entwicklungs- und Beschaffungsprozessen berücksichtigen.
- **Change-Management**: Freigabe von betrieblich relevanten Änderungen durch den bDSB sicherstellen.

Die Prozesse, in denen Löschmaßnahmen als Umsetzungsvorgabe definiert, implementiert und überwacht werden, sind festzulegen. Dafür sollen möglichst bereits vorhandene Prozesse angepasst werden. Auch die Fortschreibung des Löschkonzepts und der Regellöschfristen sind festzulegen. Formale Festlegungen für Verantwortung und Prozesse sind notwendig. Mindestens genauso wertvoll ist aber ein konstruktives Klima, in dem der Datenschutzbeauftragte, die fachlichen Anwender und die betrieblich Verantwortlichen zusammenarbeiten.[11]

In der Leitlinie werden auch Empfehlungen für die Dokumentationsstruktur gegeben. Demnach entstehende Dokumente sind das Löschkonzept selbst sowie das Dokument „Regellöschfristen“. In letzterem werden die Löschklassen und die Datenarten mit ihren Löschregeln beschrieben. Alle weiteren Dokumente sollen wie vergleichbare Dokumente in der Dokumentenlandschaft der verantwortlichen Stelle eingeordnet werden, beispielsweise Umsetzungsvorgaben für Querschnittsbereiche als Richtlinien. Wo es sich anbietet, können Inhalte auch in bestehenden Dokumenten ergänzt werden, beispielsweise Umsetzungsvorgaben für Einzelsysteme in System- oder Betriebshandbüchern oder Löschregeln für Papierakten in Mitarbeiter-Handbüchern.

Ein Löschkonzept zu etablieren, stellt eine verantwortliche Stelle vor einige Herausforderungen. Daher gibt die Leitlinie auch Hinweise für ein Projekt „Löschkonzept“.

3.4 Abgrenzung der Leitlinie

Die Leitlinie ist fokussiert auf die Elemente eines Löschkonzepts und den Prozess der Einführung. Folgende Aspekte werden nicht betrachtet:
- Konkrete Löschregeln und Löschfristen. Diese hängen von den jeweils einschlägigen Rechtsvorschriften und den zulässigen Zwecken der Verarbeitung durch die jeweilige verantwortliche Stelle ab.
- Technische Mechanismen zur Löschung und deren Sicherheitsniveau. Dazu liegen bereits eine Reihe von Standards und Anleitungen vor, die den Umgang mit klassifizierten Informationen regeln.
- Daten, die keinen Personenbezug aufweisen. Allerdings kann die Vorgehensweise grundsätzlich auch auf solche Datenbestände übertragen werden.

4 Nutzen der Leitlinie

Die Leitlinie bietet umfangreichen Nutzen. Unternehmen, die personenbezogene Daten verarbeiten, können für ihr eigenes Löschkonzept auf einer Vorgehensweise für effiziente Löschprojekte aufsetzen. Sie können damit die Löschung personenbezogener Daten rechtskonform gestalten.

Daneben bietet ein Löschkonzept für die verantwortliche Stelle viele weitere Vorteile. Der Lebenszyklus von Daten wird für die Definition der Löschregeln vom Ende, nämlich vom Zeitpunkt ihrer Beseitigung her gedacht. Dadurch entstehen Anregungen, Prozesse „aufzuräumen“. Das gilt auch für die zu löschenden Datenbestände: Damit Löschfunktionen umgesetzt werden können, müssen Datenschiefstände bereinigt werden. Datenbestände werden verkleinert – das kommt der Performanz von Datenbanken zu Gute. Und schließlich sparen Migrationsprojekte viel Aufwand, wenn sie sich nicht um historische Formate, Altbestände oder andere Restbestände kümmern müssen, die inzwischen gelöscht werden konnten.

Techniker werden der Frage der Löschung in Beschaffungs- und Entwicklungsprojekten sowie im Betrieb höheren Stellenwert einräumen. Die Anforderungen an Produkte und Dienstleister können klar strukturiert formuliert werden.

5 Ausblick

Wenn viele Unternehmen die gleiche Vorgehensweise und die gleichen Begriffe verwenden, könnten sich mittel- bis langfristig branchenspezifisch übertragbare Datenarten und Löschregeln etablieren. Würden diese von den Aufsichtsbehörden akzeptiert, ergäbe sich für die jeweils verantwortliche Stelle hohe Rechtssicherheit im Hinblick auf ihre Löschpflichten. Die Aufsichtsbehörden verfolgen die Arbeiten daher mit Interesse.

Für die Entwicklung neuer Infrastrukturen, beispielsweise E-Mobility oder Smart Grid, werden Datenschutzaspekte einen hohen Stellenwert besitzen. Mit Hilfe der Leitlinie könnten die beteiligten Akteure bereits in sehr frühen Phasen einheitliche Löschregeln für die personenbezogenen Datenbestände festlegen.

Eignung für die internationale Standardisierung

Der Nutzen der Leitlinie für den Datenschutz wäre noch größer, wäre sie als internationaler Standard etabliert. Der Stellenwert von Löschfunktionalitäten in Produkten würde erhöht. Hersteller, die die Umsetzung eines Löschkonzepts systematisch unterstützen, könnten Marktvorteile erwarten. Die Begriffsbildung in einem Standard würde auch die Kommunikation zwischen Kunden und Auftraggebern wie auch intern beim Hersteller erleichtern. Derzeit bemühen wir uns deshalb, auf der Basis der Leitlinie ein internationales Standardisierungsprojekt bei ISO zu etablieren.

6 Referenzen

Für wertvolle Hinweise zu diesem Beitrag danke ich Herrn Reinhard Fraenkel und Frau Karin Schuler.

[ISO/IEC 29001]	ISO/IEC 29100 - International Organization for Standardization / International Electrotechnical Commission (2011): ISO/IEC 29100 - Information technology - Security techniques - Privacy framework, ISO/IEC, 2011.
[Fraenkel/ Hammer 2007]	Fraenkel, R. / Hammer, V. (2007): Rechtliche Löschvorschriften, DuD 12/2007, 899 ff.; http://www.secorvo.de/publikationen/rechtliche-loeschvorschriften-fraenkel-hammer-2007.pdfa
[Hammer/ Fraenkel 2007]	Hammer, V. / Fraenkel, R. (2007): Löschkonzept, DuD 12/2007, 905 ff.; http://www.secorvo.de/publikationen/loeschkonzept-hammer-fraenkel-2007.pdf
[Hammer/ Fraenkel 2011]	Hammer, V. / Fraenkel, R. (2011): Löschklassen - standardisierte Fristen für die Löschung personenbezogener Daten, DuD 12/2011, 890 ff.; http://www.secorvo.de/publikationen/loeschklassen-hammer-2011.pdf.
[Hammer/ Schuler 2012]	Hammer, V. / Schuler, K. (2012): Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Secorvo, Karlsruhe, 2012; http://www.secorvo.de/publikationen/din-leitlinie-loeschkonzept-hammer-schuler-2012.pdf.

1 Die Toll Collect GmbH ist die Betreiberin des deutschen Mautsystems.

2 [Fraenkel/ Hammer 2007], [Hammer/ Fraenkel 2007], [Hammer/ Fraenkel 2011]. Zu Erfahrungen bei der Umsetzung eines Löschkonzeptes siehe auch Fraenkel in diesem Heft.

3 Das Programms „Innovation mit Normen und Standards“ wird vom Bundesministerium für Wirtschaft und Technologie gefördert. Projektträger ist das DIN.

4 [Hammer/ Schuler 2012]

5 Beteiligt waren z. B. Daimler AG, Deutsche Bahn AG, TÜV Informationstechnik GmbH, SAP AG, Swiss Reinsurance Company Ltd., der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und das Unabhängige Landeszentrums für Datenschutz Schleswig-Holstein.

6 Die Datenarten sind mindestens so aufzuteilen, wie es rechtlich unterschiedliche Verwendungszwecke gibt. Es spricht aber nichts dagegen, weitere fachliche Aspekte zu berücksichtigen und eine feinere Aufteilung vorzunehmen. Dadurch kann z. B. dem Sprachgebrauch der Anwender für ihre Datenbestände Rechnung getragen werden.

7 [Hammer/ Fraenkel 2011]

8 Selbstverständlich können keine beliebigen Kompromisse gewählt werden. Beispielsweise ist im Falle einer Auswahlentscheidung zwischen zwei Fristen die kürzere zu wählen. Die Wahl von Standardlöschfristen muss auch vor der Aufsichtsbehörde vertreten werden können.

9 Die Typen sind: Zeitpunkt der „Erhebung der Daten“, „Ende eines Vorgangs“ und „Ende der Beziehung zum Betroffenen“.

10 Die Grafik wurde übernommen aus [Hammer/ Schuler 2012].

11 Siehe dazu auch Fraenkel in diesem Heft.

Reinhard Fraenkel / Volker Hammer

Erfahrungen bei der Umsetzung eines Löschkonzeptes

1 Einleitung

Die Toll Collect GmbH ist die Betreiberin des Mautsystems in Deutschland. Da es hinsichtlich der im Rahmen der Mauterhebung anfallenden Fahrt- und Kontrolldaten klare Löschgebote im Bundesfernstraßenmautgesetz (BFStrMG) gibt, waren die sich aus dem BFStrMG ergebenden Löschfristen schon seit 2005, dem Zeitpunkt des Mautstarts, erfolgreich umgesetzt. Das Löschen personenbezogener Daten war damit von Anfang an Teil der Kultur des Unternehmens.

Für andere Arten personenbezogener Daten gelten die Löschgebote des § 35 Abs. 2 Nr. 3 BDSG. Konsequenter Weise wurde das Löschkonzept daher weiterentwickelt. Jetzt sind Löschregeln auch für die anderen im normalen Geschäftsablauf der Toll Collect GmbH anfallenden Arten personenbezogener Daten festgelegt. Die zugehörigen Löschmaßnahmen wurden inzwischen für die datenhaltenden Systeme umgesetzt.

In diesem Beitrag berichten wir über Erfahrungen aus dem Umsetzungsprojekt.

2 Erforderlichkeit und Löschen

Das BDSG fordert die Löschung personenbezogener Daten, wenn die weitere Speicherung der Daten für ein Unternehmen nicht mehr erforderlich ist. Leider lässt der Gesetzgeber die wenigen Rechtsanwender, die diese Vorschrift ernst nehmen, weitgehend allein, wenn es darum geht, die Norm des § 35 Abs. 2 BDSG mit Leben zu füllen. Es wäre beispielsweise schon viel gewonnen, wenn das BDSG hinsichtlich der Löschfristen das insbesondere für die Privatwirtschaft wenig taugliche Kriterium der Erforderlichkeit mit etwas mehr Kontur füllen könnte. Leider ist es in der Regel bereichsspezifischen Datenschutzregelungen vorbehalten, Löschgebote so zu konkretisieren, dass sie auch für den Rechtsanwender umsetzbar und überprüfbar werden.

Die Unbestimmheit der Norm darf aber nicht dazu führen, sie erst gar nicht zu beachten. Das Löschgebot reflektiert nämlich in besonderer Weise das informationelle Selbstbestimmungsrecht und den Grundsatz des Verbotsgesetzes mit Erlaubnisvorbehalt. Einmal rechtmäßig erhobene personenbezogene Daten müssen gelöscht werden, wenn die weitere Speicherung der Daten für die verantwortliche Stelle nicht mehr erforderlich ist. Diesen Zeitpunkt zu bestimmen ist damit die Aufgabe der verantwortlichen Stelle.

3 Voraussetzungen für die Umsetzung

Voraussetzung für die Implementierung von Löschregeln ist, dass diese Regeln vor Beginn des Umsetzungsprojekts definiert sind. Die Fristbestimmung für die Löschung der verschiedenen Arten personenbezogener Daten, die im Geschäftablauf der Toll Collect GmbH anfallen, wurde durch das Datenschutzteam angestoßen. In Abstimmung mit den Fachbereichen des Unternehmens und unter Beachtung der Gesetze, die spezielle Aufbewahrungspflichten auch für personenbezogenen Daten vorschreiben, wie beispielsweise dem HGB oder der AO, wurden die erforderlichen Speicherfristen der Datenarten bestimmt und dementsprechend die Löschregeln festgelegt.[1] Im Falle der Toll Collect werden die Löschregeln im Dokument „Regellöschfristen“ zusammengefasst.

Durch die Festlegung von Löschregeln für Datenarten wird von konkreten IT Systemen abstrahiert. Damit gelten einheitliche Fristen für alle Bestände einer Datenart. Um die Löschregeln für die einzelnen Datenarten festzulegen, wurde ein System von Löschklassen entwickelt.[2] Dadurch kann leicht verglichen werden, ob Datenarten mit ähnlichen Zwecken auch gleich behandelt werden. Außerdem wird die Zuweisung der Löschregeln viel effizienter – ein wichtiger Erfolgsfaktor für das Löschkonzept. Durch einen umfangreichen Review-Prozess und über Workshops mit den Fachbereichen, die Daten verwenden, wurden die Löschregeln abgestimmt.

Am Ende des Prozesses stand ein von der Geschäftsführung freigegebenes Dokument „Regellöschfristen“ mit unternehmensweiter Gültigkeit. Zugleich wurde die datenschutzkonforme Löschung personenbezogener Daten in den Katalog der Unternehmensziele aufgenommen. Die Toll Collect GmbH hat damit § 35 Abs. 2 Nr. 3 BDSG erfolgreich mit Leben gefüllt. Vermutlich sind einige der Löschregeln auf andere Unternehmen übertragbar, weil viele der betrachteten Datenbestände, wie Kundenstammdaten oder Buchhaltungsdaten, auch in jedem anderen Unternehmen anfallen.

Mit der Freigabe einher ging der Beschluss der Geschäftsführung, ein Projekt zur Umsetzung der Regellöschfristen aufzusetzen. Projektanforderer war der betriebliche Datenschutzbeauftragte. Die Projektverantwortung lag beim Fachbereichsleiter Betrieb zentrale Systeme. Er ist nach den Regelungen der Toll Collect der Datenverantwortliche für die meisten Systeme und damit auch für die Umsetzung und die betriebliche Überwachung von Löschmaßnahmen verantwortlich. Er etablierte seinerseits ein kleines Projektteam, das die Anforderungen des Dokumentes „Regellöschfristen“ in für die Entwicklung der Löschprozeduren taugliche Pflichtenhefte transformierte und die weiteren Projektarbeiten koordinierte.

4 Motivation zum Löschen

Auf die gute Ausgangsbasis für das neue Löschprojekt wurde unter 1. schon hingewiesen. Die Löschung der sensiblen Maut- und Kontrolldaten im deutschen Mautsystem war schon zu Beginn des produktiven Betriebs des Mautsystems erfolgreich in die Unternehmensprozesse integriert worden. Durch die so gewachsene Löschkultur war die Notwendigkeit der Löschung personenbezogener Daten sowohl der Geschäftsführung als auch den Fachbereichen klar. Das erleichterte die Definition der Regellöschfristen wie auch der Pflichtenhefte. Lästige Grundsatzdiskussionen mussten nicht mehr geführt werden. Vielleicht bietet es sich auch für andere Unternehmen an, die Umsetzung eines Löschkonzepts mit einem „Leit-Datenbestand" zu beginnen. Selbstverständlich war auch der Beschluss der Geschäftsführung für Umsetzung eine zentrale Voraussetzung der weitgehend reibungslosen Umsetzung.

Der Erfolg eines solchen Projektes hängt, das ist eine gewonnene Erkenntnis, ganz wesentlich an der Person des Projektleiters. Er muss teamfähig sein und offen für Argumente. Er muss unterschiedliche Standpunkte verstehen und, wo es notwendig ist, Kompromisse finden und sie den betroffenen Stakeholdern vermitteln. Er muss, um es auf einen Nenner zu bringen, den Erfolg wollen und von der Sinnhaftigkeit der Datenlöschungen überzeugt sein. Das alles ist keine Selbstverständlichkeit. All diese Vorraussetzungen waren in der Person des konkreten Projektleiters erfüllt. Da er im Bereich des Systembetriebs tätig ist, motivierten ihn – ganz unabhängig von einer datenschutzgerechten Löschung – zusätzlich die betrieblichen Vorteile einer durchgängigen Löschung der Daten. Nach der Produktivsetzung der Löschmechanismen würden in einzelnen Systemen bis ca. 30% der Datenvolumina gelöscht sein. Das würde zu einem stabileren Systembetrieb und zu verbesserter Performance der Systeme führen. Auch mit betriebwirtschaftlichen Vorteilen konnte gerechnet werden. Diese Erwartungen erwiesen sich neben der Tatsache, dass die Umsetzung des Löschkonzepts zu einem der Unternehmensziele erklärt worden war, als ein großer Motivationsschub für die Umsetzung. Sie halfen dann auch über gelegentlich aufflammende Diskussionen über das Löschen an sich oder über einzelne Löschfristen mit den anwendenden Fachbereichen hinweg.

Diese Diskussionen hatten gelegentlich, jedenfalls für das Datenschutzteam auch erheiternde Momente. Ein Beispiel sind die Diskussionen mit dem Data-Warehouse-Team. Das Team hatte Anonymisierungsstrategien für ein Data-Warehouse-System (DWS) erarbeitet. Gäbe es nur das Data Warehouse, wären diese Strategien auch ausreichend gewesen. Aber dies wäre eine verkürzte Sicht der Dinge gewesen, denn selbstverständlich hängt die Beurteilung der Frage einer hinreichenden Anonymisierung wesentlich auch von der Systemlandschaft ab, in die das DWS eingebettet ist. Da wo unternehmensweit Zusatzwissen in anderen Systemen gespeichert ist, das eine Deanonymisierung ermöglicht, müssen höhere Anforderungen an den Grad der Anonymisierung gestellt werden. Dementsprechend mussten die Anonymisierungsstrategien im DWS weiter geschärft werden. Das Datenschutz-Team beteiligte sich aktiv an diesem Prozess und konnte in der gemeinsamen Diskussion schnell die relevanten Attribute identifizieren.

Dieses Beispiel steht stellvertretend für andere ähnlich gelagerte Diskussionen. Sie sind immer der Mühe wert, denn so werden die Ansätze des Datenschutzes argumentativ in die Breite des Unternehmens getragen. Das Datenschutz-Team wird so im Unternehmen als Anreger und als Gestalter statt als Verhinderer wahrgenommen.

5 Technische Umsetzung

Ein Löschkonzept kann gut ausgearbeitet sein, es steht aber zunächst nur auf dem Papier. Durch das Konzept alleine wird kein Datensatz und keine Tabelle in einer Datenbank gelöscht. Für die Systeme müssen Löschmaßnahmen entwickelt und vor allem getestet werden.

Die Löschroutinen mussten in eine bestehende Systemlandschaft integriert werden. Insofern war die Situation der Toll Collect GmbH sicherlich vergleichbar mit der Situation vieler anderer Unternehmen. IT-Landschaften entwickeln im Laufe der Zeit eine hohe Komplexität. In den gewachsenen Strukturen gibt es immer auch Brüche oder unerwartete Abhängigkeiten zwischen Datenbeständen. Solche Abhängigkeiten können bei der Löschung von Daten zu Fehlfunktionen für einzelne Prozesse führen. Daher mussten im Umsetzungsprojekt des Löschkonzepts vom Projektteam

- einerseits die Datenarten in den Beständen der einzelnen Systeme identifiziert werden, um die Löschregeln zuweisen zu können und
- andererseits die Abhängigkeiten der Systeme untereinander genau überprüft werden und für die relevanten Datenarten jeweils ein führendes System bestimmt werden.

Beispielsweise müssen bestimmte Daten nach einiger Zeit nur noch auf Grund handels- oder steuerrechtlicher Vorschriften aufbewahrt werden. Da die Daten aber in unterschiedlichen Systemen verwendet werden, musste entschieden werden, ob es nicht genügt, die Daten dann nur noch in einem System vorzuhalten – mit der Konsequenz, dass sie in den anderen Systemen gelöscht werden können. Die Frage kann zunächst theoretisch entschieden werden, bedarf aber in jedem Fall der gründlichen praktischen Überprüfung, um unbeabsichtigte Nebeneffekte auszuschließen.

Aber auch aus anderen Gründen sollte im Rahmen der Umsetzung des Löschkonzepts die gesamte Systemlandschaft noch einmal intensiv analysiert werden. Denn auch bei einer sehr gut gepflegten, alle Changeprozesse berücksichtigenden Systemdokumentation kann es Lücken geben. Verdeckte Abhängigkeiten der Prozesse untereinander können sich im Laufe der Jahre eingeschlichen haben. Es können auch bisher unbemerkt gebliebene Datenschiefstände zwischen verschiedenen Systemen bestehen. Erkannt werden können diese Probleme, soweit sie nicht schon bekannt sind, vor allem in der Phase des Testens. Der Phase kommt daher im Rahmen eines solchen Entwicklungsprojekts sehr große Bedeutung zu. Die finale Löschung der Daten ist irreversibel. Daher muss durch die Analyse der Systemlandschaft und der Einzelsysteme sowie durch das Testen sichergestellt werden, dass durch

die Produktivsetzung der Löschroutinen die normalen Arbeitsabläufe nicht gestört werden. Die vertiefte Analyse und die intensive Phase des Testens waren Teile des Projekts bei der Toll Collect GmbH. Die dabei identifizierten Probleme konnten sowohl technisch wie datenschutzrechtlich vertretbar gelöst werden.

Spätestens an diesem Punkt bekommen viel früher getroffene Grundsatzentscheidungen hinsichtlich der eingesetzten IT-Systeme noch einmal unerwartete Relevanz. Aus der Sicht des Löschprojekts bestehen nämlich die folgenden Kernanforderungen an IT-Systeme:

- Unterstützung differenzierter Löschung im Datenbestand: Löschregeln für verschiedene Datenarten enthalten unterschiedliche Fristen. Enthält der Datenbestand eines Systems unterschiedliche Datenarten – was in der Regel der Fall ist – müssen differenzierte Löschregeln zur Anwendung kommen.
- Archivieren und Sperren: Nach Möglichkeit sollen aufbewahrungspflichtige Daten nur in einem System gespeichert werden. Spätestens im Löschprojekt muss daher entschieden werden, in welchem System aufbewahrungspflichtige Daten vorgehalten werden. Diese Daten sollen dann aber im Sinne des BDSG für die normalen Anwender gesperrt sein. Das Vorhalten der aufbewahrungspflichtigen Daten soll die produktiven Systeme möglichst wenig belasten – es ist sinnvoll, sie zu archivieren (im Sinne von auszulagern).
- Wechselwirkungen mit gelöschten Daten von führenden Systemen ausschließen: Die Systeme, in denen die Daten vor dem Ende der Aufbewahrungspflicht gelöscht werden, sollen mit den verbleibenden Daten korrekt weiterarbeiten.
- Löschmöglichkeit in Archiven: Schließlich muss auch die Löschung von archivierten Daten möglich sein.

Nicht jede der Kernanforderungen ist für jedes System relevant. Aber die Systemlandschaft insgesamt mit ihren Wechselwirkungen zwischen den Systemen muss die Anforderungen abdecken. Nur dann, wenn die relevanten Systeme über geeignete Implementierungen der Anforderungen verfügen, kann unabhängig von den eingesetzten Ausgangsprodukten entschieden werden, ob die Archivierung der Daten beispielsweise im CRM-System erfolgen soll oder im Buchhaltungssystem. Werden in einem der üblichen Kandidaten für die Archivierung, beispielsweise CRM, DMS oder Buchhaltungssystem Anforderungen nicht abgedeckt, wird der Lösungsraum des Löschprojekts eingeschränkt.

Wenn in einem System die notwendigen Funktionen zunächst gar nicht vorgesehen sind, wie dies beispielweise für Archivierung/Sperrung bei PeopleSoft-basierter CRM-Software der Fall ist, scheidet dieses System für die Archivierung in aller Regel aus. Denn schon das in diesem Fall erforderliche individuelle Customizing des Produkts würde die Kosten der Umsetzung eines Löschkonzepts erheblich in die Höhe treiben.

Noch prekärer wird die Situation natürlich dann, wenn Systeme in ihrer Ursprungskonfiguration überhaupt keine Löschfunktionalitäten vorsehen, wie dies beispielsweise lange im SAP R/3 HR der Fall war.[3] Für diesen Umstand wurde seitens SAP zunächst im Wesentlichen technische Gründe ins Feld geführt, aber auch die Auffassung der Industrie, Datenschutz dürfe kein Geld kosten. Inzwischen besteht im SAP eine deutlich besserer Ausgangssituation. Beispielsweise werden bei Toll Collect in den Modulen BWS, FI, CO und PA personenbezogene Daten mit Hilfe der Archivierungsfunktionen ausgelagert und gesperrt. Die Löschung erfolgt dann für archivierte Daten. Diese Funktionskette wird auch zum Löschen von Daten mit kurzen Fristen genutzt: Die Speicherdauer der Archivdateien ist dann auf wenige Tage reduziert. Um keinen falschen Eindruck zu bezüglich andere Software-Produkte zu erwecken: Auch PeopleSoft beispielsweise ist für durchgängiges Löschen nicht gut vorbereitet und erfordert erhebliche Customizing-Aufwände.

Die oben genannten Kernanforderungen lenken den Blick aber auf die Beschaffungsprozesse von Software. Unabhängig von der gesetzlich gebotenen Vorabkontrolle, die ja nur für bestimmte Anwendungen verpflichtend ist, muss sichergestellt werden, dass bereits im Beschaffungsprozess von Software die datenschutzrechtlichen Anforderungen an IT gestützte Verfahren berücksichtigt werden. Dazu gehört zwingend, dass zu entwickelnde Software oder Standardsoftware über die notwendigen Lösch-, Archivierungs- oder Anonymisierungsfunktionalitäten verfügen und Wechselwirkungen, die Löschen verhindern, ausgeschlossen werden.[4]

6 Lessons learned

Nach Abschluss des Projektes sind in allen dafür vorgesehen Systemen die Löschfunktionalitäten implementiert und produktiv gesetzt, unter anderem im Data-Warehouse, dem CRM-System und in SAP. Im DWS wurden bei Produktivsetzung knapp 30% des Datenbestandes gelöscht, in den SAP-Modulen 25% und im CRM-System ca. 15%.

Mit den jetzt etablierten Löschroutinen werden künftig alle Datenbestände mit Löschfristen länger als einem Jahr jährlich bereinigt, Datenbestände mit kürzeren Löschfristen meist wöchentlich. Die Performance der angepassten IT-Systeme hat sich deutlich verbessert. Zukünftig notwendige Datenmigrationen werden allein wegen der geringeren Menge vorgehaltener Daten und wegen konsistenterer Datenhaltung kostengünstiger. So wird auch der ökonomische Nutzen von Datensparsamkeit transparent.

Der Praxistest für ein übergreifendes Löschkonzept darf als gelungen betrachtet werden. Drei Elemente waren im Projekt Voraussetzung für die erfolgreiche Umsetzung.

1. Verantwortung und Unterstützung der Geschäftsführung:

Ohne einen entsprechenden Rückhalt in der Geschäftsführung ist ein Projekt „Löschkonzept“ nicht möglich. Die Geschäftsführung muss die Löschregeln und das Projektbudget freigeben. Sie muss das Projekt fördern und fordern – wozu sie gesetzlich verpflichtet ist.

2. Vollständigkeit der Regellöschfristen:

Es war sehr hilfreich für den Projektverlauf, dass die Regellöschfristen zum Start des Umsetzungsprojekts weitge-

hend vollständig und im Unternehmen abgestimmt waren. Nur so können die Anforderungsdokumente für die Umsetzung von Anfang an die richtigen Regeln vorgeben. Jede nachträglich identifizierte Datenart und jede angepasste Löschregel erfordert mindestens ein neues Review der geänderten Regellöschfristen durch die betroffenen Fachbereiche. Und erst danach können die Anforderungsdokumente fertiggestellt und freigegeben werden. Dadurch steigt die Projektkomplexität erheblich und die Motivation der Beteiligten sinkt stark.

3. Interaktion zwischen Datenschutz-Team und den weiteren Beteiligten des Unternehmens:

Selbstverständlich kann ein solch übergreifendes Projekt nicht „glatt durchgezogen" werden. Dazu gibt es einerseits zu viele unterschiedliche Interessen im Unternehmen und andererseits zu viele Überraschungen in den technischen Zusammenhängen. Das Datenschutz-Team kann sich deshalb nicht zurücklehnen, sondern muss das Projekt aktiv begleiten. Es muss motivieren und gemeinsam mit den anderen nach Kompromissen suchen, wenn Lösungsansätze komplex, teuer oder unpraktikabel scheinen. Dafür ist es sehr hilfreich, wenn im Datenschutz-Team juristische und technische Kompetenz vertreten ist. Das Datenschutz-Team sollte sich als Technikgestalter verstehen.

7 Ausblick

Die Erstellung und Umsetzung eines Löschkonzepts ist keine einmalige Aufgabe. Die Weiterentwicklung von Geschäftsprozessen, Änderungen der Rechtsvorschriften und die Veränderungen an IT-Systemen erfordern eine kontinuierliche Fortschreibung. Zukünftige Weiterentwicklungen der IT-Systeme bei Toll Collect müssen die Anforderungen der Regellöschfristen bruchlos unterstützen. Diese Vorgaben für die technische Umsetzung und die Dokumentation der Löschmaßnahmen werden bereits in den Pflichtenheften berücksichtigt.

Mit Interesse verfolgt die Toll Collect GmbH, dass eine verallgemeinerte Beschreibung der Vorgehensweisen in der Standardisierung aufgegriffen wurde.[5] Eine ISO-Norm würde dem Thema sowohl bei Technikern in Entwicklung und Betrieb als auch in anwendenden Fachbereichen erhebliches, zusätzliches Gewicht verleihen. Wenn viele Unternehmen ein entsprechendes Löschkonzept verwenden, sind auch Synergieeffekte zu erwarten: viele Datenarten und Löschfristen sind sicher zwischen Unternehmen einer Branche übertragbar.

Diese allgemeinen Löschregeln liefern auch den Herstellern wertvolle Vorgaben: sie könnten sich nicht mehr darauf zurückziehen, dass keine Anforderungen bestünden. Vielmehr müssten sie endlich Systeme so gestalten, dass sie mit geringem Aufwand datenschutzgerecht eingesetzt werden können. Von den Aufsichtsbehörden sollten solche Entwicklungen durch klare Empfehlungen für datenschutzfreundliche Softwareprodukte unterstützt werden.

1 Zu den näheren Einzelheiten der Regellöschfristen und der Methodik der Fristbestimmungen vgl. Hammer/ Fraenkel, Löschklassen, DuD, 12/2011, S 890 ff, mit weiteren Literaturhinweisen; Hammer, Löschen nach Regeln, in diesem Heft; und ausführlich Hammer, V. / Schuler, K. 2012: Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Secorvo, Karlsruhe, 2012; http://www.secorvo.de/publikationen/din-leitlinie-loeschkonzept-hammer-schuler-2012.pdf..

2 Vgl. dazu näher Hammer/ Fraenkel DuD 12/2011.

3 Erst auf Druck der Aufsichtsbehörden hat SAP Löschfunktionalitäten in SAP HR integriert. Vgl. dazu instruktiv: 23. Tätigkeitsbericht des BfDI 2009- 2010 S. 61. Vgl. zur gleichen Problematik auch 36. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (2007) Nr. 5.10.3.2; 38. Tätigkeitsbericht (2009) Nr. 4.8.3; 39. Tätigkeitsbericht (2010) Nr.4.1.5 und 40. Tätigkeitsbericht (2011) Nr. 3.10.3.

4 Die Aufsichtsbehörden könnten das Ihrige dazu tun, wenn nicht nur versteckt in Tätigkeitsberichten Hinweise auf datenschutzfreundliche Tools zu finden wären. Wünschenswert wäre ein Weißbuch, in dem datenschutzfreundliche Softwaresysteme aufgelistet wären. Eine Software, die beispielsweise keine Löschfunktionalitäten vorsieht, dürfte im Geltungsbereich des BDSG nicht vertrieben werden. Die Entwicklung bei SAP HR hat gezeigt, wie von den Aufsichtsbehörden zum Nutzen des Datenschutzes erfolgreich Druck auf Anbieter aufgebaut werden kann.

5 Siehe dazu Hammer, Löschen nach Regeln, in diesem Heft.

Cartoon



Hajo Köppen

Vertrauliche Papierunterlagen vernichten: DIN-Konfetti ist Pflicht



Zur traditionellen Thanksgiving-Parade in New York leistete auch die dortige Polizei letztes Jahr einen Beitrag und ließ Konfetti regnen. Allerdings stellte sich nach dem Konfettiregen heraus, dass es sich bei den Papierschnipseln um nur grob geschredderte Polizeiunterlagen handelte. Auf einigen der Schnipsel waren Sozialversicherungsnummern und die Namen von Polizisten zu erkennen.[1]

Aber man muss nicht unbedingt über den großen Teich schauen, um auf solche Datenpannen zu stoßen. „Patientenakten im Sperrmüll" titelte die TAZ im März 2012. Deutschlands größter privater Krankenhauskonzern Asklepios, der allein in Hamburg zehn Kliniken betreibt, hatte höchst sensible Patientenakten, u.a. Notfallberichte und Abrechnungsberichte mit Tausenden von personenbezogenen Daten kistenweise im Sperrmüllcontainer entsorgt. Einen Versuch des datenschutzgerechten Schreddern hatte die Klinik erst gar nicht unternommen.[2]

Im August 2011 fanden sich im normalen Restmüll eines Berliner Vereins für Sozialberatung detaillierte Berichte zu psychischen und physischen Erkrankungen, über Missbrauch, Verwahrlosung und Betreuungsbedarf, alle Unterlagen mit Namen und Anschriften der Betroffenen, Lebensläufen, Zeugnissen, Briefen und ärztlichen Befunden.[3]

Es bedarf sicher keiner weiteren Ausführungen, dass zumindest die beiden letzten Fälle mit dem Datenschutzrecht, insbesondere mit den Vorschriften zur Datensicherheit und zum Datengeheimnis, nicht im Einklang stehen.

Datenträger, egal ob Papier, CD, Festplatte oder USB-Stick, die personenbezogene Daten enthalten und entsorgt werden können, dürfen nicht einfach in der Mülltonne „gehauen" werden. Sie müssen datenschutzgerecht zerkleinert werden. Was bei der datenschutzgerechten Vernichtung von Datenträgern zu beachten ist, wird in dem Faltblatt „Datenschutz-Tipp 4" der Technischen Hochschule Mittelhessen (THM) beschrieben, in dem die neue DIN 66399 (Büro- und Datentechnik - Vernichtung von Datenträgern) berücksichtigt wird. Die neue DIN ersetzt seit Oktober 2012 die alte DIN 32757 und legt genaue Anforderungen an die ordnungsgemäße Datenträgervernichtung fest. Bei Papier etwa die Größe des „Konfettis", je nach Sicherheitsstufe. Das Faltblatt ist abrufbar unter: www.thm.de/datenschutz/datenschutztipps.

1 Süddeutsche Zeitung, NYPD lässt Konfetti aus vertraulichen Daten regnen, 27.11.2012.

2 Die Tageszeitung, Patientenakten im Sperrmüll, 3.03.2012.

3 Die Tageszeitung, Datenschutz im Eimer, 7.08.2011.

Hans-Hermann Schild

Datenlöschung in SAP - Wo liegt das Problem?

Ein Beitrag zur Löschroutine

Art. 12 Buchst. b) EU-Datenschutzrichtlinie 95/46/EG (DS-RiLi) regelt, dass der von der Verarbeitung (Erhebung, Verarbeitung und Nutzung nach dem Sprachgebrauch des Bundesdatenschutzgesetzes BDSG) Betroffene die Löschung von Daten fordern kann, deren Verarbeitung nicht den Bestimmungen der Richtlinie entsprechen. Die Löschung führt dazu, dass der Verantwortliche der Verarbeitung nicht mehr über die personenbezogenen Daten verfügt. Dabei ist es gleichgültig, ob die Löschung durch Überschreiben oder gar Vernichten des Datenträgers erfolgt. Damit besteht immer ein Löschanspruch, wenn die Voraussetzungen für eine rechtmäßige und damit zulässige Datenverarbeitung entfallen sind. Das ist insbesondere der Fall, wenn die Daten nicht mehr erforderlich sind.

Daher regelt § 4 e Satz 1 Nr. 7 BDSG, dass im Rahmen der Meldung von Verfahren mit personenbezogenen Daten auch die Regelfristen für die Löschung der Daten aufzunehmen sind. Insoweit hat eine datenverarbeitende Stelle (Betrieb oder Behörde) festzulegen, wann welche Daten im Regelfall gelöscht werden, weil sie nicht mehr erforderlich sind. Jedoch gibt es – wenn auch in nur sehr wenigen Fällen – die Entscheidung des Bundes- oder Landesgesetzgebers, wann welche Daten zu löschen sind. Um die Löschung bei großen Datenmengen personenbezogener Daten gewährleisten zu können bedarf es einer entsprechenden Löschroutine, die die technische Umsetzung der Vorgaben aus einem Löschkonzept darstellt. Damit gehört das Löschen auch zu den Maßnahmen der Datensicherheit.

1. Löschfristen und -vorgaben

Die Beamtengesetze des Bundes und der Länder regeln, welche Personaldaten wie lange aufzubewahren sind. So regelt z.B. § 107e Abs. 2 Hessisches Beamtengesetz (HBG), dass Mitteilungen in Strafsachen, soweit sie nicht Bestandteil einer Disziplinarakte sind, sowie Auskünfte aus dem Bundeszentralregister mit Zustimmung des Beamten nach drei Jahren zu entfernen und zu vernichten sind. In § 107f Abs. 2 HBG ist bestimmt, dass Unterlagen über Beihilfen, Heilfürsorge, Heilverfahren, Unterstützungen, Erholungsurlaub, Erkrankungen drei Jahre und über Umzugs- und Reisekosten sechs Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, aufzubewahren sind. Unterlagen, aus denen die Art einer Erkrankung ersichtlich ist, sind unverzüglich zurückzugeben oder zu vernichten, wenn sie für den Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden. Über § 34 Abs. 1 Satz 2 Hessisches Datenschutzgesetz (HDSG) finden diese Vorschriften in Hessen auch für Arbeiter, Angestellte usw., also alle Beschäftigten im öffentlichen Dienst, Anwendung, auch wenn diese ansonsten nicht unter das Hessische Beamtengesetz fallen. Damit ist für die Beschäftigten kraft Gesetzes festgelegt, welche Daten wie lange erforderlich sind und damit rechtmäßig gespeichert werden dürfen, auch wenn die Personaldaten elektronisch verarbeitet werden.

2. Einführung von SAP in Hessen

Im Jahre 1999 beschloss die damalige Hessische Landesregierung zur Umstellung des Haushalts-, Kassen- und Rechnungswesens auf die doppelte Buchführung mit Kosten- und Leistungsrechnung, Produktsteuerung, ergebnisorientierter Budgetierung und entsprechendem Controlling landesweit verbindlich die SAP-Software R/3 einzusetzen. Im Jahre 2002 folgte dann die Einführung des HR-Moduls der Software SAP R/3 (Personalwesen, mit den Kernfunktionen Personaladministration, Personalabrechnung, Stellenwirtschaft, und Organisationmanagement). Dabei wurde im Schulbereich mit der Pilotphase begonnen und im Jahre 2003 die Hessische Polizei einbezogen.

Hierbei rügte zunächst der Hauptpersonalrat der Hessischen Polizei die Verletzung seiner Beteiligungsrechte, später die Personalräte der einzelnen Polizeidienststellen (Polizeipräsidium, LKA, usw.). Insoweit hatte sich die Fachkammer für Personalvertretungsrecht Land beim Verwaltungsgericht Wiesbaden mit der Einführung von SAP R/3 HR aus personalvertretungsrechtlicher Sicht zu befassen.

3. Entscheidungen des VG Wiesbaden

Nach den Personalvertretungsgesetzen ebenso wie nach dem Betriebsverfassungsgesetz hat der Personalrat die Aufgabe, darüber zu wachen, dass die zugunsten der Beschäftigten geltenden Gesetze, Verordnungen, Tarifverträge, Dienstvereinbarungen und Verwaltungsanordnungen durchgeführt werden. Das Überwachungsrecht des Personalrats erstreckt sich auch auf die Vorschriften von BDSG und HDSG. Die Datenschutzgesetze schützen auch die auf die Beschäftigten bezogenen persönlichen Daten, die bei der einzelnen Dienststelle gespeichert sind oder dort anderweitig verarbeitet werden. Sie sind Rechtsvorschriften „zugunsten der Mitarbeiter“, auch wenn sie nicht speziell dazu bestimmt sind, die Beschäftigten des öffentlichen Dienstes vor Missbrauch personenbezogener Daten zu schützen. Das Überwachungsrecht des Personalrats gibt ihm aber lediglich die Befugnis, bei dem Dienststellenleiter auf die Beachtung der begünstigenden Vorschrift hinzuwirken (BVerwG, Beschluss vom 26.03.1985,

Az.: 6 P 31/82). Insoweit zog das Gericht im Rahmen der Amtsermittlung das Verfahrensverzeichnis nach § 6 HDSG (die Meldung im Sprachgebrauch des BDSG) bei und prüfte die Einhaltung datenschutzrechtlicher Vorgaben.

Dabei führte das Gericht u.a. aus: *„Entscheidender dürfte vielmehr jedoch sein, dass es derzeit bei dem Modul SAP R/3 HR keine Löschroutine gibt und insoweit die Angaben in dem Verfahrensverzeichnis über die Fristen über die Löschung gemäß § 19 Abs. 3 HDSG unter allgemeinen Hinweis über die Fristen auf die entsprechenden gesetzlichen Aufbewahrungsvorschriften des Landes Hessen nicht nur dürftig, sondern gänzlich unvollständig sind. Dies auch, wenn nach dem Bekunden des sachverständigen Zeugen G. es insoweit einen Arbeitsauftrag an die Arbeitsgruppe „Archivierung" gibt, welche ein Konzept für die Löschung und Archivierung der Daten erarbeiten soll, ein solches derzeit jedoch nicht besteht. Mithin kann derzeit eine ordnungsgemäße automatisierte Verarbeitung personenbezogener Daten der Beschäftigten in keiner Weise gewährleistet werden."* (Beschluss vom 4.10.2004, Az. 23 L 2121/04).

In einem weiteren Verfahren weist das Gericht auf die Bedeutung des Verfahrensverzeichnisses (der Meldung) hin. Hiernach ist Sinn und Zweck eines Verfahrensverzeichnisses, dass sich die verantwortliche Stelle vor der Anschaffung und Implementierung eines automatisierten Verfahrens zur Verarbeitung von personenbezogenen Daten Gedanken macht, wie die im Hessischen Datenschutzgesetz vorgegebenen Umgangsregelungen mit personenbezogenen Daten auch der Beschäftigten umgesetzt und beachtet werden. § 10 Abs. 2 Satz 1 HDSG regelt, dass ein Verfahren auszuwählen oder zu entwickeln ist, welches geeignet ist, so wenig personenbezogene Daten zu verarbeiten, wie dies zur Erreichung des angestrebten Zweckes erforderlich ist (entspricht § 3 a BDSG – Datenvermeidung und Datensparsamkeit). Hierzu gehört auch die Gewährleistung der Löschung von Daten. „Dies ist vorliegend hinsichtlich der erforderlichen Löschung ganz offensichtlich in keinster Weise erfolgt. Ob und inwieweit auch bereits Daten gespeichert worden sind, welche schon zu löschen sind, konnte in der mündlichen Verhandlung zwar nicht geklärt werden und auch der Beteiligte konnte hierzu keinen sachdienlichen Beitrag leisten, hierauf kommt es aber nicht an." (VG Wiesbaden, Beschlüsse vom 23.05.2005, Az. 23 LG 560/05 (V), RDV 2005, 177-179; Az. 23 LG 511/05, ZfPR online 2007, Nr 1, 17-18; Az. 23 LG 485/05 (V), DuD 2005, 427-433).

Zur Überraschung der Kammer konnte auch keiner der Beteiligten dem Gericht erklären, wer für diese Vorabkontrolle nach § 7 Abs. 6 Satz 1 HDSG die Verantwortung trägt. Insgesamt kam das Gericht zu dem Ergebnis, dass das für die Einführung der automatisierten Datenverarbeitung aufgrund des Systems SAP R/3 HR vorliegende Musterverfahrensverzeichnis nach § 6 HDSG (Version 12/2004) derart erhebliche Mängel offenbart, dass in verfassungswidriger Weise in das Grundrecht des Beschäftigten auf informationelle Selbstbestimmung gem. Art 2 Abs 1 i.V.m. Art 1 Abs. 1 Grundgesetz (GG) eingegriffen wird (Hier: fehlendes Löschkonzept, Verarbeitung von Gesundheitsdaten, fehlende schriftliche Fixierung der Verantwortlichkeit für die Vorabkontrolle, ungeklärtes Zugriffskonzept, keine Klärung der Auswertung und Aufbewahrung von Protokollen; insgesamt ist eine rechtmäßige Datenverarbeitung der Daten der Beschäftigten derzeit nicht gewährleistet.).

In einem letzten Beschluss zu SAP führte dann das Gericht aus, *„dass im Falle einer rechtswidrigen Datenverarbeitung – welche die Kammer aufgrund der mündlichen Verhandlung vom 13.05.2005 festgestellt hat – jeder Beschäftigte einer jeden Dienststelle die Möglichkeit hat, entsprechenden gerichtlichen Rechtsschutz zu beantragen, da seine personenbezogenen Daten nicht auf rechtmäßige Weise verarbeitet werden (vgl. Art. 6 Abs. 1 Buchstabe a) EG-Datenschutzrichtlinie)"*

4. Folgen aus den Entscheidungen

Der Hessische Datenschutzbeauftragte stellte in seinem 36. Tätigkeitsbericht vom 12.02.2008 daraufhin fest, dass die Löschung von Daten im SAP-Standard nicht vorgesehen ist. Ihm sei jedoch durch die Projektleitung immer wieder versichert worden, dass die Löschung von Daten bei SAP thematisiert und spätestens drei Jahre nach der erstmaligen Speicherung von Daten (Zeitpunkt, an dem die Aufbewahrungsfrist für die Krankheits- und Urlaubsdaten endet und diese nach § 107f Abs. 2 HBG zu löschen sind) eine entsprechende Löschroutine zur Verfügung stehen werde. Da die Löschung eines der zentralen Datenschutzrechte ist, hätte bereits eine ordnungsgemäß durchgeführte Vorabkontrolle nach § 7 Abs. 6 HDSG das Ergebnis erbringen müssen, dass das Verfahren so nicht eingesetzt werden darf (Ziffer 5.10.3.2 - Löschung von Daten im SAP R/3 HR-System12.02.2008). Damit wurden die Ausführungen des Verwaltungsgerichts Wiesbaden bestätigt.

In seinem 39. Tätigkeitsbericht vom 15.03.2011 stellte der Hessische Datenschutzbeauftragte fest, dass die Fristen für die Löschung von Urlaubs- und Krankheitsdaten im SAP R/3 HR-System des Landes Hessen und die einschlägigen Vorschriften zur Löschung von Daten (§ 107f HBG, §§ 19 Abs. 3 und § 34 Abs. 4 HDSG) nicht eingehalten werden und die vorgeschriebenen Löschungen von Krankheits- und Urlaubsdaten nicht erfolgt sind (Ziffer 4.8.3 - Löschung von Daten in SAP R/3 HR); um dann im 40. Tätigkeitsbericht vom 3.08.2012 festzustellen, dass zwar eine Löschroutine zum Löschen von krankheits- und urlaubsbedingten Abwesenheiten am 7. April 2011 produktiv gesetzt wurde, jedoch eine Auswertung der SAP-Datenbank ergeben habe, dass am 1. November 2011 noch insgesamt 7.559 Personaldatensätze gespeichert waren, bei denen die urlaubs- und krankheitsbedingten Daten aus der Zeit vor dem 31. Dezember 2006 noch nicht gelöscht worden waren. Insoweit handelt es sich hierbei um einen nicht unerheblichen Verstoß gegen die Vorschriften des § 107f Abs. 2 HBG (Ziffer 3.10.3 - Löschung von Daten im SAP R/3 HR-System). Mithin ist immer noch keine ordnungsgemäße Löschroutine vorhanden. Dies hat auch der Bundesdatenschutzbeauftragte bei der Bundesverwaltung festgestellt (23. Tätigkeitsbericht 2009-2010, Ziffer 5.4 - Einmal erfasst – für immer gespeichert? Probleme mit der Datenlöschung). Er hat dies mit der Aussage verknüpft, dass für den Fall, dass sich keine Änderung ergibt,

er dem Einsatz von SAP-Produkten in Zukunft nicht mehr befürworten könne.

5. Fazit

Bei der ersten Datenverarbeitung hat die Meldung (das Verfahrensverzeichnis) vollständig vorzuliegen (EuGH, Urteil vom 09.11.2010, Az. C-92/09 mit Anm. von Schild in „Das Gewerbearchiv“ GewArch 2011, S. 24, 28 f.). Sind die Löschroutine und die damit verbunden Löschfristen nicht erfasst, ist das Verfahren als Ganzes rechtswidrig. Dies hat zur Folge, dass rechtswidrig gespeicherte Daten ohne inhaltliche Unterscheidung sofort und vollständig zu löschen sind. Behörden und Unternehmen gehen insoweit bei der Nutzung und Anwendung von Verfahren, die über keine ausreichende Löschroutine verfügen, ein hohes wirtschaftliches Risiko ein, von möglichen Bußgeldern ganz zu schweigen.

Merke: Nicht alles, was auf dem Markt angeboten wird, ist rechtlich erlaubt. Die Verantwortung für Datenschutzkonformität trägt weiterhin die verantwortliche Stelle.



digitalcourage e.V.





Erfolg beim Meldegesetz: Vermittlungsausschuss kippt Widerspruchslösung

Berlin, 26.2.2013. Das Bündnis „Meine Daten sind keine Ware“ begrüßt das Ergebnis des Vermittlungsausschusses zum Meldegesetz. Nach dem heutigen Beschluss sollen Meldedaten künftig nur noch mit Einwilligung der Bürgerinnen und Bürger weitergegeben werden dürfen. Die Zweckbindung wurde gestärkt. Kritisch beurteilt das Bündnis weiterhin, dass auch Unternehmen Einwilligungen einholen können.

Das Bündnis „Meine Daten sind keine Ware“ begrüßt das Ergebnis des heutigen Vermittlungsausschusses zum Meldegesetz. „Breiter Bürgerprotest hat dazu geführt, dass die datenschutzfeindliche Regelung des Bundestages gekippt wurde“, sagt Susanne Jacoby von Campact. Künftig sollen Meldedaten zu Zwecken der Werbung und des Adresshandels nur noch mit Einwilligung der betroffenen Person herausgegeben werden dürfen. Ebenfalls positiv bewerten die im Bündnis vertretenen Organisationen, dass die Zweckbindung bei Melderegisterauskünften gestärkt wurde. Adressdaten müssen nun nach Erfüllung des Übermittlungszwecks gelöscht werden.

Der Bundestag hatte im Juni 2012 beschlossen, dass Daten von Bürgern grundsätzlich herausgegeben werden dürfen, wenn diese dem nicht widersprochen haben. Der Bundesrat stoppte daraufhin das Gesetz. Bundestag und Bundesrat müssen dem nun vorgelegten Vorschlag des Vermittlungsausschusses noch zustimmen.

Nach Ansicht des Bündnisses besteht jedoch noch ein Manko: Die Einwilligung in die Herausgabe von Meldedaten kann auch von demjenigen Unternehmen eingeholt werden, das die Meldedaten anfordert. Dieses Verfahren öffnet Tür und Tor für erschlichene oder behauptete Einwilligungen. Das tatsächliche Vorliegen einer Einwilligung müssen die Meldebehörden lediglich stichprobenhaft kontrollieren. „Damit bleibt eine Hintertür für missbräuchliche Datenabfragen offen“, kritisiert Rena Tangens von Digitalcourage.

„Der Protest der Verbraucher hat erneut gezeigt, dass sie gefragt werden wollen, wenn ihre Daten für Marketing genutzt werden. Daher sollte nicht nur bei Meldedaten, sondern grundsätzlich, wenn personenbezogene Daten zu Werbezwecken verwendet werden, eine Einwilligung des Betroffenen eingeholt werden müssen“, ergänzt Florian Glatzner vom Verbraucherzentrale Bundesverband (vzbv).

Haben Bürger sowohl beim Meldeamt als auch gegenüber Unternehmen Willenserklärungen abgegeben, ist außerdem vollkommen unklar, welche davon in Zweifelsfällen gelten soll.

„Jetzt ist es deshalb an jedem Einzelnen, die Meldebehörde davon in Kenntnis zu setzen, wenn man die Abfrage seiner Daten nicht erlauben möchte“, ergänzt Karin Schuler von der Deutschen Vereinigung für Datenschutz e.V. „Irgendwann könnte sonst jeglicher Überblick verloren gehen, wem man Einwilligungen erteilt oder entzogen hat. Wenn das Gesetz keine transparenten Regeln schafft, muss jeder Einzelne eben nachhelfen.“

Das Bündnis wird getragen vom Kampagnennetzwerk Campact, dem Verbraucherzentrale Bundesverband, dem Datenschutz- und Bürgerrechtsverein Digitalcourage (vormals FoeBuD) und der Deutschen Vereinigung für Datenschutz. Den Online-Appell der Kampagne haben insgesamt mehr als 200.000 Menschen unterzeichnet. Mehr Informationen zur Kampagne: www.campact.de/melderecht

Wann ist ein Nein ein Nein?

Der vehemente Protest von Bürgerrechtlern und Datenschützern war schließlich erfolgreich. Im Bündnis „Meine Daten sind keine Ware“ hat sich die DVD zusammen mit digitalcourage (vormals FoeBud), vzbv und campact gegen den Kahlschlag beim Melderecht eingesetzt. Über 200.000 Unterschriften wurden gegen den ungefragten Verkauf von Meldedaten durch die Meldeämter gesammelt. Bundesrat und Vermittlungsausschuss haben schließlich den durch den Bundestag verursachten datenschutzrechtlichen GAU abgemildert. Es ist keine Musterlösung, die da erzielt wurde, aber ein Kompromiss, der Schlimmeres verhindert hat.

Bei dem folgenden Text handelt es sich um den Nachdruck eines Gastkommentars, den Karin Schuler für die Mittelbayerische Zeitung verfasst hat.

Der zügellose Verkauf von Meldedaten ist vom Tisch.

Besonders verbraucherfreundlich ist das neue Gesetz dennoch nicht.

Wie oft muss ich zukünftig bekräftigen, dass die Meldebehörde meine Daten nicht verkaufen soll? Im besten Fall gar nicht – dann nämlich, wenn ich mich nicht rühre. Das ist die gute Nachricht. Und das nur, weil sich Bürgerrechtsverbände vernehmlich gegen den ursprünglich geplanten, freien Verkauf von Meldedaten eingesetzt haben.

Die schlechte ist: habe ich jemals Einwilligungen erteilt, wird es kompliziert. Nicht aus Sicht des Gesetzgebers, aber für mich. Denn zukünftig kann ich meinen Willen an vielen Stellen erklären. Ob meine Meldedaten zu Marketingzwecken verkauft werden dürfen, kann ich sowohl der Meldebehörde als auch interessierten Unternehmen mitteilen. Dabei stellt die Einwilligung bei der Meldebehörde eine generelle Erklärung dar; gegenüber anderen gilt sie nur für das jeweilige Unternehmen. Genauso verhält es sich mit Widerrufen. Mein Einwilligungs- und Widerrufsmanagement wird also zukünftig zu einer herausfordernden Aufgabe. Transparenz – als eines der wesentlichen Datenschutzprinzipien – sieht anders aus.

Dabei wäre es so einfach gewesen: Die Meldebehörde als Halterin der Daten hätte Einwilligungen und Widersprüche zentral verwalten können. Stattdessen können Unternehmen nun Meldedaten abfragen, wenn sie behaupten, hierfür Einwilligungen der Betroffenen zu besitzen. Die Behörde soll die Richtigkeit der Behauptung nur stichprobenartig überprüfen. Man ist kein Hellseher, wenn man die Chance als gering einschätzt, erschlichene oder gar nicht vorhandene Einwilligungen zu entdekken. In einem Hintergrundpapier des Verbraucherzentrale Bundeverbandes wird die hohe Dunkelziffer untergeschobener Einwilligungserklärungen thematisiert. Es taugt eben nicht, wenn man den Bock zum Gärtner und die Werbeindustrie zum Verwalter datenschutzrechtlicher Einwilligungen macht.

Was lerne ich als mündige Verbraucherin daraus? In erster Linie dies: Sorge, so gut es geht, für Dich selbst! Erlaube den Abgleich mit Meldedaten erst gar nicht. Und achte darauf, was Du unterschreibst. Außerdem: teile dem Meldeamt vorsorglich mit, dass Du einem Abgleich niemals zustimmen wirst. Die Behörde ist nämlich zur Prüfung verpflichtet, wenn sie Anhaltspunkte für Unregelmäßigkeiten hat. Und dies wäre der Fall, würde ein Unternehmen dennoch behaupten, meine Einwilligung vorliegen zu haben.

Aber nicht nur der faule Kompromiss beim Datenverkauf befremdet im neuen Gesetz. Was, glauben Sie, haben Mieter und Hotelgäste gemeinsam? Der Gesetzgeber scheint beiden nicht über den Weg zu trauen! Übernachte ich auf Reisen nicht privat, macht mich dies offenbar verdächtig. Ich muss dem Hotelier einen Meldeschein ausfüllen, damit die Behörde meine Reiseroute bequem nachvollziehen kann. Als Mieter bin ich wohl noch unglaubwürdiger. Während jeder Hausbesitzer sich ohne Umstände selbst anmelden kann, benötige ich als Mieter die bestätigende Unterschrift meines Vermieters. Wird man durch Grundbesitz zum vertrauenswürdigeren Menschen? Das Bild, das der Gesetzgeber in Teilen des Meldegesetzes von Bürgerinnen und Bürgern zeichnet, scheint aus sehr vergangenen Zeiten zu stammen.

Never ending story…

Schon im zweiten Anlauf versuchte die schwarz-gelbe Koalition zum Jahreswechsel ein Gesetz zum Beschäftigtendatenschutz durchzubringen, das seinen Namen nicht verdiente. Unter dem Deckmantel der Verhinderung heimlicher Videoüberwachung wurde eine nur leicht geänderte Textversion vorgelegt, die die Rechte von Beschäftigten massiv einschränken sollte und die Zugriffsmöglichkeiten auf ihre Daten ausweitete. Bereits der damalige Entwurf fiel durch und die dann ergänzten Flickschustereien machten ihn nicht besser. Die Eile, mit der er durch den Bundestag gebracht werden sollte, stieß auf breiten Protest von Bürgerrechtlern und Datenschützern.

Die DVD beteiligte sich zusammen mit dgitalcourage, FIfF und campact an einer Protestaktion, in deren Verlauf innerhalb weniger Tage 70.000 Menschen einen Online-Appell gegen dieses Gesetz unterschrieben. Die Beratung über den Entwurf wurde schließlich im Innenausschuss und im Bundestag von der Tagesordnung genommen – angeblich war man von der Heftigkeit des Protests überrascht und wollte sich zunächst erneut mit Verbändevertretern beraten.

Nach erneuten Gesprächen der Koalition mit Arbeitgebern und Gewerkschaften wurden die Pläne endgültig schließlich aufgegeben. In dieser Legislaturperiode ist also kein Beschäftigtendatenschutzgesetz mehr zu erwarten und ein Vergleichbares hoffentlich auch in Zukunft nicht.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Massive Zunahme von behördlichen Kontodatenabfragen

Behörden überprüfen immer mehr Privatkonten: Die Abfragen sind 2012 um 15,5% auf 72.578 gestiegen. Seit 2008 hat sich damit die Zahl mehr als verdoppelt. Als das automatisierte Abrufverfahren für Stammdaten wie Name, Geburtsdatum oder Adresse der Bankkunden 2005 eingeführt wurde, lagen die Abfragen noch bei 8.689. Seitdem sind sie um rund 830% gestiegen. Im Dezember 2011 gingen noch durchschnittlich 136 Anfragen pro Arbeitstag beim Bundeszentralamt für Steuern ein, im Dezember 2012 waren es 481. Bei der Abfrage erfahren die Sicherheits-, Finanz- und Sozialbehörden die Stammdaten zu den Konten, die ein Person besitzt. Das jeweilige Kreditinstitut, das die Stammdaten verwaltet, bemerkt zunächst von der behördlichen Online-Abfrage nichts. Dadurch soll verhindert werden, dass die Bank misstrauisch wird und negative Schlüsse, z. B. über die Kreditwürdigkeit des Kunden, zieht. Ergibt sich aus der Abfrage ein Verdacht, z. B. weil sich darunter ein Konto befindet, dass von dem Betroffenen nicht angegeben wurde, so kann konkret bei der Bank nachgehakt werden.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Peter Schaar verlangte, die Abfragen müssten wieder zur Ausnahme werden: „Ich fordere die Bundesregierung auf, den Umgang mit der Kontodatenabfrage einer ergebnisoffenen wissenschaftlichen Überprüfung zu unterziehen. Auch eine verbesserte Begründungspflicht könnte dazu führen, dass die Zahl der Abfragen eingedämmt wird.“ Abfragen sollten nur noch in Frage kommen, wenn konkrete Anhaltspunkte für Steuerhinterziehung, Sozialbetrug oder erhebliche Straftaten vorlägen. Routineabfragen seien schon nach der heutigen Rechtslage nicht erlaubt. „Derzeit erfährt der Betroffene häufig noch nicht einmal von der Abfrage.“ Da bereits bei der Kontoeröffnung die Stammdaten automatisch als Datensatz gespeichert werden und somit über das Abrufverfahren zur Verfügung stehen, erfolge „letztlich eine anlasslose Erfassung grundsätzlich aller Kontoinhaber in Deutschland“. Die Handhabung in den einzelnen Bundesländern sei sehr unterschiedlich. Seit dem 01.01.2013 können auch Gerichtsvollzieher Kontodatenabfragen durchführen (Kuhr, Das Ende des geheimen Kontos, SZ 15.01.2013, 25; Behörden überprüfen immer mehr Privatkonten, www.augsburger-allgemeine.de 14.01.2013).

Bund

Mehr Akteneinsichtsanträge bei Stasi-Unterlagen-Behörde

Mehr als zwei Jahrzehnte nach dem Ende der DDR ist das hohe Interesse an den Stasi-Unterlagen im Jahr 2012 um 10%, und damit noch einmal kräftig gestiegen. 2012 gingen 88.231 Anträge auf Akteneinsicht bei der Stasi-Unterlagen-Behörde ein, im Jahr zuvor waren es 80.611. Seit 2002 schwanken die Zahlen zwischen knapp 95.000 und gut 80.000. Mittlerweile können auch Kinder, Brüder oder Schwestern Anträge auf Einsicht in Akten ihrer toten Eltern oder Geschwister stellen. Diese machen etwa 6% aller Anfragen und 10% der Erstanträge aus. Seit 1992 wurden rund 6,8 Mio. Anträge auf Akteneinsicht gestellt. Zur Akteneinsicht für Forschung und Medien wurden 1.430 Anträge registriert. Etwa 5.500 Ersuche zur Rehabilitation von damals politisch Verfolgten wurden gestellt.

Die Stasi-Überprüfungen von Beschäftigten im öffentlichen Dienst nahmen – auf niedrigem Niveau – ebenfalls zu, von 210 auf 317. Das im Herbst 2011 geänderte Stasi-Unterlagen-Gesetz ermöglicht Stasi-Überprüfungen im öffentlichen Dienst bis 2019. Auch die Stasi-Gedenkstätte Berlin-Hohenschönhausen meldet steigende Besucherzahlen. 2012 seien rund 351.000 Menschen gekommen, das waren 10.000 mehr als 2011. Während die meisten Besucher aus Westdeutschland und westeuropäischen Ländern anreisten, kamen aus Ostdeutschland und Berlin nur 28.000 und damit 2.000 weniger als im Vorjahr.

Der Vorsitzende des Beirats der Stasi-Unterlagen-Behörde, Richard Schröder, begrüßte das steigende Interesse an den Stasi-Akten. Offenbar gehe die Entwicklung auf die Wissbegier der nächsten Generation zurück. Schröder mahnte jedoch: „Wir müssen verhindern, dass mit dem Interesse auch die Wartezeiten steigen. Das drohe jetzt. „Viele Anträge haben Experten zufolge damit zu tun, dass die Distanz zur Vergangenheit ausreichend groß geworden ist und die Konfrontation damit als weniger schmerzlich gilt.“

Der Obmann der CDU / CSU-Bundestagsfraktion im Ausschuss für Kultur und Medien, Marco Wanderwitz, erklärte: „Wir haben eine Verstetigung auf hohem Niveau und hier und da ein paar Zuwächse. Das bestätigt mich darin, dass die Entscheidung, die Zukunft der Behörde langfristig zu sichern, richtig war. Jedes weitere Jahr, in dem das Interesse bestehen bleibt, bringt ein Stück Zukunftssicherung für die Behörde.“ Dies gelte womöglich auch über 2019 hinaus. Der kulturpolitische Sprecher der FDP-Bundestagsfraktion, Reiner Deutschmann, äußerte sich ähnlich: „Ich könnte mir vorstellen, dass

die Behörde ihre Eigenständigkeit auch über 2019 hinaus behält.“ Man könne die Akten nicht archivieren wie x-beliebige andere. Inoffiziell herrscht Konsens unter Politikern und Fachleuten, dass die Behörde 2019 schließen soll. Sicher ist das nicht. Behörden-Chef Roland Jahn hält den Zeitpunkt offen (Stasi-Unterlagen-Behörde, PE 04.01.2013, Interesse an Stasi-Akten auch 2012 ungebrochen; Decker, Das Interesse an Stasi-Akten wächst, www.mz-web.de 04.01.2013).

Bund

Finanzministerium zwingt LKW-Fahrer zur Klo- und Duschdoku

In einem zweiseitigen Schreiben an die obersten Finanzbehörden der Länder legt das Bundesfinanzministerium fest, wie die etwa 1,5 Millionen deutschen LKW-FahrerInnen die Kosten für Toilettengänge oder das Duschen auf Raststätten in ihren Steuererklärungen ansetzen müssen. Eine einfache Schätzung soll nicht ausreichen. Vielmehr müssen die FahrerInnen eine Art Toilettenfahrtenbuch führen, also ihre Klo- und Duschpraxis sowie die Kosten hierfür akribisch notieren und möglichst alle Belege sammeln. Daraus berechnet das Finanzamt einen Durchschnittswert für die täglichen Bedürfnisse, der für alle Fahrtentage dann in die Steuererklärung eingeht.

Uwe Rauhöft vom Neuen Verband der Lohnsteuerhilfevereine (NVL) kritisiert diese Vorgaben als „ein irrsinnig aufwändiges Verfahren“. Bisher hatten viele Finanzämter eine Schätzung für diese Kosten anerkannt. Noch im März 2012 hatte der Bundesfinanzhof (BFH) geurteilt, dass geschätzte fünf Euro für die täglichen „Reisenebenkosten“ der LKW-FahrerInnen durchaus akzeptabel seien. Nun müssen die FahrerInnen von ihrem Aufwand sogar den Wert der Bons abziehen, die sie an Raststätten oder Autohöfen bekommen. Autohöfe verlangen oft für eine Übernachtung eine Standgebühr von 10 bis 15 Euro, wobei in diesem Preis meist ein Gutschein fürs Essen enthalten ist. Weil es dafür aber eigene steuerliche Pauschalen gibt, erkennen viele Finanzämter die Quittungen nicht an. Deshalb wiederum erstatten einige Speditionen den FahrerInnen diese Kosten nicht (Jalsovec, Fahrtenbuch fürs Klo, SZ 22./23.12.2012, 31).

Baden-Württemberg

Sicherheitstechnik von Bosch in China

Die International Campaign for Tibet (ICT) wirft dem schwäbischen Technologieriesen und Autozulieferer Bosch vor, chinesischen Gefängnissen gezielt Sicherheits- und Überwachungstechnik anzubieten. China sei ein autoritär regierter Staat ohne unabhängige Justiz, kritisierte Kai Müller, Sprecher der Menschenrechtsorganisation. Angesichts der Repression in dem Land, in dem der Friedensnobelpreisträger Liu Xiaobo in einem chinesischen Gefängnis sitzt und Tibeter sich aus Protest gegen Repressionen anzünden, sei „eine solche Geschäftstätigkeit in China beschämend“. Ein Werbespruch des schwäbischen Stiftungskonzerns mit einem Jahresumsatz von 50 Mrd. Euro ist: „Vertrauen Sie uns, wenn es um ihre Sicherheit geht.“

Bosch bewirbt auf seiner chinesischsprachigen Webseite unter anderem mit Kurzvideos seine Produkte „AutoTrack“ und „AutoDome“. Dabei handelt es sich um eine moderne Überwachungskameratechnik speziell für Gefängnisse und Sicherheitseinrichtungen, die Bewegungen erkennt und Verdächtige auf Schritt und Tritt verfolgen kann. In einem Werbevideo des Konzerns wird ein animierter Clip präsentiert, in dem ein Wärter einen Häftling im orangefarbenen Overall in einen Raum mit einer Glasscheibe zur Besuchszeit führt. Als sich der Gefangene setzt, heißt es im chinesischen Untertitel: „Überwachen Sie die Unterhaltung zwischen Besuchern und Häftlingen. Legen Sie fest, wie lange die Kommunikationskanäle geöffnet sind.“ Anfang Dezember 2012 fand in Peking die „Security China 2012“ statt, eine vom Ministerium für Öffentliche Sicherheit organisierte Messe, die von chinesischen Sicherheits- und Justizbehörden besucht wird, wo Bosch für seine Techniken warb. Im Messekatalog hieß es, die Messe solle „alle Ebenen der Sicherheit in der Volksrepublik China verbessern.“

ICT forderte Bosch auf, den Vertrieb von Gefängnisausrüstung in China unverzüglich einzustellen und Auskunft darüber zu geben, wie viele chinesische Gefängnisse Bosch bislang ausgerüstet hat. Insbesondere will ICT wissen, ob Techniken des Unternehmens auch in Gefängnissen in Tibet zum Einsatz kommt. Eine Sprecherin der Bosch-Sicherheitssysteme GmbH erklärte daraufhin: „Wir haben kein chinesisches oder tibetisches Gefängnis mit unseren Sicherheitsprodukten ausgestattet.“ Bei den Filmen auf der Webseite handele es sich um Trailer, „die wie vieles andere Werbematerial zentral erstellt und dann in viele unterschiedliche Sprachen übersetzt“ worden seien. Angesprochen werden sollten mit der chinesischen Webseite auch Länder wie Singapur und Taiwan, in denen ebenfalls Chinesisch gesprochen werde. Die Sprecherin betont, dass Bosch ein werteorientiertes Unternehmen sei. Dazu zähle auch die Einhaltung der Menschenrechte. Sie dementierte nicht, dass Bosch seine Überwachungstechnik nach China verkaufen will, wenn dortige Gefängnisse sie haben wollen. Bosch betont, man halte alle embargorechtlichen und außenwirtschaftlichen Vorschriften ein und habe „daher keine grundsätzlichen Bedenken, in China wirtschaftlich aktiv zu sein“. Bosch wirke durch sein Engagement vor Ort sogar an der positiven Weiterentwicklung der chinesischen Wirtschaft und Gesellschaft mit. Die Technik werde zudem nicht direkt Gefängnissen oder Behörden angeboten, sondern an Elektronikhändler vor Ort verkauft; wem diese die Produkte weiterverkaufen, könne Bosch nicht kontrollieren.

Wolfgang Büttner von der Menschenrechtsorganisation Human Rights Watch meinte: „Wenn Überwachungstechnologie für Gefängnisse an Länder verkauft wird, in denen rechtsstaatliche Standards verletzt werden und Personen willkürlich festgehalten werden, dann verletzen Unternehmen die notwendige Sorgfaltspflicht. Die Europäische Union verhängte nach der blutigen Niederschlagung der Demokratiebewegung 1989 in Peking ein Waffenembargo gegen China. Überwachungstechnik fällt aber nicht dar-

unter. Die Bundesregierung kritisierte wiederholt die drakonischen Strafen gegen Dissidenten und Menschenrechtsverteidiger in der Volksrepublik. Kai Müller von ICT kritisierte, europäische Unternehmen würden in China immer häufiger durch Anbiederung und sogar durch Komplizenschaft mit dem Regime in Peking auffallen. Unternehmen wie Bosch seien verpflichtet, menschenrechtliche Prinzipien zu achten und zu fördern: „Wenn Bosch chinesische Gefängnisse mit seiner Technik umwirbt, trägt das Unternehmen Mitverantwortung für Menschenrechtsverletzungen in China. An der Verantwortlichkeit des Unternehmens ändert auch nichts der Verweis auf Elektronikhändler oder zwischengeschaltete Personen.“ Bosch müsse das Geschäftsfeld in China einstellen. Die Bosch-Gruppe machte 2011 in China 6,7 Milliarden US-Dollar Umsatz, wobei zur Produktpalette auch vieles mehr als Sicherheitstechnik gehört: Bremssysteme, Fahrassistenten für Autos, Bohrmaschinen und Staubsauger. Damit zählt die Volksrepublik zu Boschs wichtigsten Märkten (Giesen/Hägler, Hochspannung, SZ 08./09.12.2012; Lee, Bosch hofiert Chinas Knäste, www.taz.de 06.12.2012).

Bayern

Ordnungsreferent bewirkt Beschlagnahmung von Nutzerdaten bei Presseorgan

Die Polizei hat am 28.01.2013 im Verlagshaus der „Augsburger Allgemeinen“ die Daten eines Forumsnutzers beschlagnahmt. Die Behörde ermittelt gegen einen User des Online-Forums dieser bayerischen Zeitung. Dieser soll den Ordnungsreferenten der Stadt, Volker Ullrich (CSU), scharf angegriffen haben. Der Nutzer hatte sich im Herbst 2012 im Leser-Forum über Ullrichs Pläne geäußert, gegen die Straßenprostitution in der Stadt vorzugehen: „Dieser Ullrich verbietet sogar erwachsenen Männern ihr Feierabendbier ab 20.00 Uhr, indem er geltendes Recht beugt und Betreiber massiv bedroht!“ Ullrichs Anwalt beschwerte sich Mitte Oktober über den Kommentar. Im Forum von augsburger-allgemeine.de seien „ehrverletzende Äußerungen über Ulrich aufgetaucht.“ Dem Ordnungsreferenten sei „Rechtsbeugung“ vorgeworfen worden. Ullrichs Anwalt verlangte daraufhin von der Redaktion, den Namen des Nutzers preiszugeben.

Nach den Bestimmungen der Zeitung müssen sich die Nutzer des Leserportals mit ihren echten Daten registrieren und anerkennen, dass sie sich in ihren Kommentaren an Recht und Gesetz halten werden. Veröffentlicht wurde nur das Pseudonym „Berndi“. Die Redaktion weigerte sich, die Daten an den Anwalt herauszugeben. Jürgen Marks, Mitglied der Chefredaktion der „Augsburger Allgemeinen“: „Wir unterstützen weder Beleidigungen noch strafrechtlich relevante Äußerungen auf unserer Plattform und sind jederzeit bereit, diese nach Prüfung zu löschen, wenn wir darauf aufmerksam gemacht werden“. Die Zeitung nehme die Meinungsfreiheit und den Schutz Nutzerdaten sehr ernst.

Die Redaktion entschied sich dazu, die Passagen über den Politiker im Leserforum zu löschen, gab die Daten des betroffenen Nutzers aber nicht heraus. Volker Ullrich erstattete daraufhin Strafanzeige. Auch nach einer Aufforderung der Augsburger Polizei, weigerte sich die Redaktion weiterhin, die Daten preiszugeben. Daraufhin rückte ein Beamter mit einem Durchsuchungs- und Beschlagnahmebeschluss des Amtsgerichts Augsburg im Verlagshaus an. Der Beamte fragte gezielt nach dem Datensatz des Nutzers und nahm diesen als Ausdruck mit. Die „Augsburger Allgemeine“ sah hierin ein Verletzung der Meinungs- und Pressefreiheit. Doch gegen den richterlichen Beschluss habe sich die Redaktion nicht wehren können. Die Zeitung kündigte an, rechtliche Schritte gegen den Durchsuchungsbeschluss zu prüfen.

Volker Ulrich schrieb bei Facebook: „Ein Ordnungsreferent muss viel Kritik einstecken! Das ist auch gut so! Aber muss man sich als Jurist den Vorwurf der ‚Rechtsbeugung‘ gefallen lassen? Ich meine nein. Das Internet ist kein rechtsfreier Raum!“ Er hatte zunächst auf seinem Facebookprofil angekündigt, die Strafanzeige gegen den Foren-Nutzer zurückzuziehen. Er wolle nicht, „dass dieses Thema stadtbestimmend wird“, und hoffe daher lediglich privat auf eine Entschuldigung des Bloggers. Wenig später löschte er den Eintrag und ersetzte ihn durch einen neuen Eintrag, in dem er die Entschuldigung zur Bedingung macht: „Ich werde meine Strafanzeige zurückziehen, wenn der User sich bei mir entschuldigt.“ Bereits im Herbst 2011 hatte Ullrich die Herausgabe von Daten eines Forennutzers von der Zeitung verlangt. Die Redaktion hatte sich damals erfolgreich geweigert, die Daten herauszugeben.

Journalistenverbände kritisierten die Durchsuchungsaktion scharf. Kalle Kaschel-Arnold von der Deutschen Journalistinnen- und Journalisten-Union (dju) in Verdi meinte: „Wir finden das einen ungeheuren Vorgang“. Das Redaktionsgeheimnis müsse gewahrt bleiben. Der Vorsitzende des Bayerischen Journalisten-Verbandes (BJV), Wolfgang Stöckel, meinte die Aktion sei „völlig überzogen. Redaktionsdurchsuchungen und Beschlagnahme-Aktionen sind ein untaugliches Mittel, um in gerichtlichen Auseinandersetzungen Meinungsäußerungen von Lesern oder Internet-Nutzern strafrechtlich verwerten zu können. Sie dienen nur dazu, die Pressefreiheit und den Informantenschutz zu unterhöhlen.“ Die Staatsanwaltschaft wies alle Vorwürfe zurück (Polizei beschlagnahmt Nutzerdaten bei „Augsburger Allgemeinen“, www.spiegel.de 29.01.2013; Journalistenverbände kritisieren Beschlagnahmeaktion, www.sueddeutsche.de 29.01.2013; Beisel/Mayr, Wer ist Berndi?, SZ 30.01.2013, 1, Medien).

Berlin

Systemadministrator verkauft sensible Daten an Pharma-Lobby

Zur Verwunderung des Bundesgesundheitsministeriums war die Apothekerszene in Berlin mit deren Lobbyisten und Verbänden stets detailliert und frühzeitig informiert über Gesetzesvorhaben, interne Schriftverkehre, vertrauliche Papiere. Egal ob es um Rabattverträge über Medikamente ging, um die Neuordnung des Arzneimittelmarkts oder die Reform

der Betriebsordnung – wann immer seit 2010 die Interessen der Pharmazeuten tangiert waren, wussten die Apotheker wie auch der Fachinformationsdienst „Apotheke adhoc" erstaunlich gut Bescheid. Noch bevor Texte im Ministerbüro vorgelegt wurden, waren sie manchmal schon wortgleich in einem pharmazeutischen Fachblatt, oft inklusive Rechtschreibfehler, nachzulesen. Dies hatte zur Folge, dass die ministeriale Leitungsebene zuletzt den eigenen MitarbeiterInnen nicht mehr traute: Am Dienstsitz Friedrichstraße 108, 10117 Berlin, so Berichte von Betroffenen, wurde verdächtigt und beschimpft. Das Datenleck, so die Vermutung, müsse „irgendwo unter uns" sein.

Im September 2012 ging ein anonymer Anruf einer Frau im Ministerium ein. Die Gerüchte gehen dahin, dass sie die Verliererin eines Beziehungsdramas war, die es nun ihrem Ex heimzahlte. Der Systemadministrator Christoph H., ein IT-Spezialist mit höchster Vertraulichkeitsstufe, hatte Zugang zur gesamten Informationstechnik (IT) des Ministeriums bis hin zum E-Mail-Account des Ministers, angestellt bei einer externen Bonner Dienstleistungsfirma, so wie das üblich ist in Bundesministerien. Die Frau erzählt, die Referatsleiter staunten, der Minister reagierte: Staatsanwaltschaft, Landeskriminalamt (LKA), Strafanzeige und Ermittlungen wegen des „Verdachts des Ausspähens von Daten und Verstoßes gegen das Bundesdatenschutzgesetz". Knapp acht Wochen lang lies man den Administrator weiterarbeiten; nur wenige Mitarbeitende des Ministeriums waren eingeweiht. Am 20.11.2012 waren sich Staatsanwaltschaft und das Kommissariat 335 („Cybercrime") des Berliner LKA sicher, dass der Spion Daten nicht nur illegal ausgespäht, sondern auch an einen Lobbyisten, Thomas Bellartz, verkauft hatte, der mit der Apothekerszene bestens vertraut ist. Bellartz war Pressesprecher der Bundesvereinigung Deutscher Apothekerverbände (ABDA). Seit September 2011 ging er eigene Wege bei einer neu gegründeten Neuspree Media mit Sitz in Berlin, einem Kommunikationsunternehmen, das auf seiner Internetseite so für sich wirbt: „Die langjährige Erfahrung unseres Teams im Gesundheitsmarkt macht uns zu Spezialisten im Healthcare-Bereich. Sie müssen uns nur fragen." Die Neuspree Media hat ihre Büroräume in demselben Gebäude wie die Agentur El Pato. Und die wiederum betreibt unter anderem das Nachrichtenportal Apotheke adhoc, einen Branchendienst für den Apotheken- und Pharmamarkt. Es erfolgten Hausdurchsuchungen in den Büros von Neuspree Media, von El Pato, bei dem IT-Mann und dem Lobbyisten.

Die Ermittler gehen davon aus, dass der Lobbyist Bellartz den IT-Mann gezielt mit dem Kopieren bestimmter Daten des Gesundheitsministeriums, vor allem aus dem Apotheken- und Pharmabereich, beauftragt hat, u. a. aus dem „Pharma"-Referat 113 des Ministeriums: E-Mail-Anhänge und Dokumente aus sogenannten „öffentlichen Ordnern", in denen Akten abgelegt werden, die gerade bearbeitet werden. Die Ermittler glauben, dass sich die beiden Männer eher zufällig kennengelernt und bereits seit März 2010 miteinander kooperiert hätten. Seitdem sei es zu Dutzenden Treffen gekommen, bei denen der Computerfachmann Bellartz Datenträger mit brisantem Material übergeben habe. Dafür soll er bar kassiert haben – angeblich „ca. 500 bis 600 Euro pro Woche", heißt es in Justizunterlagen. Als Motiv für den mutmaßlichen Datenklau vermuten die Fahnder wirtschaftliche Interessen. Der IT-Mann habe mit seinem Job zwar etwa 3.000 Euro brutto verdient, aber erhebliche finanzielle und private Probleme gehabt, u. a. wegen einer bevorstehenden Scheidung.

Die ABDA wies alle Spionagevorwürfe zurück: „Es war nie und es wird nie Politik unseres Hauses sein, die Interessen der deutschen Apothekerschaft per Scheckbuch zu vertreten." Die ABDA werde alles tun, um den Sachverhalt aufzuklären und biete den Ermittlungsbehörden jede erdenkliche Unterstützung an: „Wir lehnen eine auf solche Weise erfolgte Informationsbeschaffung strikt ab und distanzieren uns davon ausdrücklich. Wir sehen mit Sorge, dass ein ganzer Berufsstand unter Generalverdacht gerät."

Der Gesundheitsexperte der Union, Jens Spahn (CDU), forderte Aufklärung von den Apotheken-Verbänden: „Wir sind ja durchaus aggressives Lobbying im Gesundheitswesen gewöhnt und können damit gut umgehen. Aber bezahlte Spionage wäre eine neue Qualität, das macht einfach nur fassungslos und wütend." Der FDP-Gesundheitspolitiker Erwin Lotter meinte, der Apothekerverband stehe in der Bringschuld. Wer lautstark seine Stimme erhebe, wenn es um die Durchsetzung höherer Honorare gehe, dürfe nicht abtauchen, wenn es um schwerwiegende Straftaten gehe und die politische Kultur dramatischen Schaden nehme.

In die besagte Zeit fielen mehrere politische Vorhaben, die finanzielle Interessen der Apothekerschaft massiv berührten. Verhandelt wurde u. a. über die Höhe des Abschlags, den die Apotheker an die Krankenkassen zahlen müssen. Er wurde in diesem Zeitraum zunächst von 2,30 Euro pro Packung auf 1,75 Euro reduziert und dann wieder auf 2,05 Euro angehoben. Die Apotheker gelten als eine der einflussreichsten Lobby-Organisationen in der Hauptstadt. Sie sind bekannt für ihr aggressives Auftreten. Minister und Abgeordnete werden bei unliebsamen Vorhaben regelmäßig mit manchmal unflätigen E-Mails und Briefen überschwemmt (Bohsem, Apotheken-Lobbyist soll Ministerium ausspioniert haben, www.sueddeutsche.de 11.12.2012; Bahr spricht von „großer Sauerei", www.sueddeutsche.de 12.12.2012; Haarhoff, Rezept für einen Krimi, www.taz.de 12.12.2012; Verdächtiger IT-Experte arbeitete auch für Ex-Umweltminister Gabriel, www.spiegel.de 16.12.2012; Das Krebsgeschwür, Der Spiegel 51/2012, 82 ff.).

Berlin

Syrischer Spion verurteilt

Das Berliner Kammergericht hat am 05.12.2012 einen Deutsch-Libanesen wegen Spionage für den syrischen Militärgeheimdienst zu zwei Jahren Haft auf Bewährung verurteilt. Das Gericht sah es als erwiesen an, dass der 48jährige von 2007 bis 2012 syrische Oppositionelle in Deutschland ausspioniert hatte. Insbesondere zu Beginn des arabischen Frühlings 2011 lieferte der Vorsitzende eines deutsch-libanesischen Freundschaftsvereins seinem Führungsoffizier viele Fotos und Informationen über RegimekritikerInnen und Demon-

strationen in Berlin (Syrischer Spion verurteilt, SZ 06.12.2012, 6).

Hessen

Innenminister wirbt für Videokontrolle

Die Videoüberwachung in Hessen leistet nach Ansicht des dortigen Innenministers Boris Rhein einen wesentlichen Beitrag zum Schutz der BürgerInnen. Im vergangenen Jahr sei die Zahl der Straftaten an videoüberwachten Plätzen und Straßen im Land um 19,5% zurückgegangen, behauptete der CDU-Politiker am 27.12.2012. 2011 wurden der Statistik zufolge an den mit Kameras überwachten Orten 1.871 Straftaten registriert. 2006 habe die Zahl noch bei fast 4.000 gelegen. Nach einem gescheiterten Bombenanschlag in Bonn war bundesweit eine Debatte um die Videoüberwachung ausgebrochen. In Hessen gibt es nach Angaben des Ministeriums derzeit 18 Videoanlagen mit 102 Kameras, von denen in der Regel die Daten sieben Tage lang gespeichert werden. 2009 seien es noch elf Anlagen mit 48 Kameras gewesen. Den stärksten Rückgang an Straftaten weise, so das Ministerium, die Konstablerwache in der Frankfurter Innenstadt auf. Seit Installation der Videoanlage im Jahr 2002 habe es fast 60% weniger Delikte gegeben. Die Drogenszene sei aufgelöst. Rhein behauptete außerdem, dass Hessen das erste Bundesland sei, das im Jahr 2000 mit der Videoüberwachung begonnen habe (Rhein wirbt für Videoüberwachung, www.fr-online.de 27.12.2012).

Mecklenburg-Vorpommern

NPD-Bundesvize muss Jugendliche wegen Persönlichkeitsverletzung entschädigen

Der stellvertretende NPD-Bundesvorsitzende Frank Schwerdt muss gemäß einem Urteil des Amtsgerichts Schwerin wegen des illegalen Filmens von Mädchen und Jungen einer Schule aus Ferdinandshof (Landkreis Vorpommern-Greifswald) insgesamt 12.000 Euro zahlen. Jede SchülerIn soll 1000 Euro bekommen. Die NeuntklässlerInnen waren mit ihrem Sozialkundelehrer vor der Landtagswahl 2011 in der Stadt zum Thema Wahlkampf unterwegs. Der Spitzenkandidat der rechtsextremen NPD, Udo Pastörs, steuerte auf die Gruppe zu und redete etwa eine halbe Stunde auf sie ein. Der Angeklagte und seine Verteidigerin waren bei dem Prozess nicht erschienen. Schwerdt, der zugleich auch Landesvorsitzender der NPD-Thüringen ist, hatte 1998 und 2000 mehrmonatige Haftstrafen unter anderem wegen Volksverhetzung und Verbreitung von NS-Propagandamaterial absitzen müssen.

Ein NPD-Aktivist filmte die Szene, später wurde das 17-Minuten-Video online gestellt. Die Eltern der Jugendlichen wurden nicht um Zustimmung gebeten. Für das Gericht war Schwerdt der presserechtlich Verantwortliche. Gegen das Urteil kann er Berufung einlegen. Nach Ansicht des Richters wurden die Jugendlichen instrumentalisiert. Auch der Lehrer der Schulklasse sei nicht schuldlos am Entstehen des NPD-Videos. Er habe nicht verhindert, dass Pastörs seine „Propagandarhetorik des Dritten Reichs“ vor den SchülerInnen ausgebreitet habe. Der Lehrer habe ihn vielmehr nach dem Motto: „Na, fragen wir ihn doch gleich mal“ regelrecht eingeladen. Die SchülerInnen hatten jeweils 2000 Euro Entschädigung verlangt. Der Anwalt der Kläger, Johannes Menting, zeigte sich dennoch zufrieden mit dem Urteil. Das Gericht habe festgestellt, dass die NPD sich nicht auf Kosten von Jugendlichen profilieren dürfe (NPD muss an Schüler zahlen SZ 01./02.12.2012, 8; NPD muss Schülern Entschädigung zahlen, www.ndr.de 30.11.2012; NPD-Bundesvize muss Jugendliche entschädigen, www.spiegel.de 30.11.2012; NPD muss Entschädigung an Jugendliche zahlen, www.lto.de 30.11.2012).

Nordrhein-Westfalen

V-Leute in der Fußballszene

Das Innenministerium Nordrhein-Westfalen (NRW) hat V-Leute in der gewaltbereiten Fußball-Fanszene eingesetzt. Gemäß einer Antwort der Landesregierung auf eine Kleine Anfrage der Piraten im Landtag waren von 2008 bis 2012 bis zu neun sog. Vertrauensleute aktiv. Es sei ausschließlich darum gegangen, Gewalt und andere schwere Straftaten zu verhindern. Bereits im Herbst 2012 hatte die Bundesregierung auf Anfrage der Linken erklärt, durch die Bundesländer würden V-Leute bei Fußball-Veranstaltungen eingesetzt. Vor NRW hatte bereits Hamburg bestätigt, dass der dortige Verfassungsschutz Links- und Rechtsextremisten auch unter Fußballfans mit V-Leuten beobachtet.

Frank Herrmann von der Fraktion der Piraten im Landtag kritisierte die Maßnahmen: „Die staatliche Kontrolle und Bespitzelung von Stadionbesuchern hat ein Ausmaß erreicht, das nicht vereinbar mit einer rechtsstaatlichen Demokratie ist. Die Maßnahmen, die gegen Fußballfans angewendet und auf Initiative der DFL (Deutsche Fußball Liga) zukünftig sogar noch verschärft werden, ähneln mittlerweile denen eines Überwachungsstaats. Der Einsatz von V-Leuten in Fangruppierungen ist unverhältnismäßig.“ Deren Einsatz solle sich auf die Bekämpfung von organisierter Kriminalität oder Terrorismus beschränken. Ähnlich kritisch äußerte sich Philipp Markhardt, Sprecher der Aktionen „ProFans“ und „12:12“: „Der Erfolg von V-Leuten darf nach Pleiten, Pech und Pannen im Zusammenhang mit der NSU bezweifelt werden. Wenn ich das lese, dann ist das eine neue Qualität, dass Fußball-Fans präventiv bespitzelt werden.“

Wolfgang Beus, Sprecher des Innenministeriums NRW, verteidigte die Maßnahme: „Es geht nicht darum, Fußball-Fans auszuspionieren oder zu bespitzeln.“ Ziel sei vielmehr, Gewalt- und schwere Straftaten zu verhindern. Der Einsatz von V-Leuten sei keine NRW-Spezialität, sondern ein allgemeines polizeiliches Mittel zur Gefahrenabwehr. Friedliche Fans sollten so geschützt werden. Die Vertrauensleute seien in der Szene und würden der Polizei Hinweise geben. Dafür erhielten sie eine Aufwandsentschädigung, in Einzelfällen auch eine Belohnung. Die Summe reiche aber in keinem Fall, um damit den Lebensunterhalt zu bestrei-

ten. Wenn die V-Leute Straftaten begingen, trenne sich die Polizei von ihnen und verfolge die Tat. Der Einsatz von V-Leuten sei überall denkbar, wo es um schwerwiegende Straftaten geht, also etwa im Rauschgiftmilieu oder in der Rockerszene (V-Leute in der Fußballszene, SZ 09.01.2013, 6; NRW lässt Fußballfans mit V-Leuten bespitzeln, www.focus.de 08.01.2013).

Nordrhein-Westfalen

Mitarbeiterüberwachung bei Aldi Süd

Ein ehemals bei Aldi Süd und Aldi Suisse tätiger Detektiv erhob schwere Vorwürfe gegen den Discounter aus Mülheim: Er habe über 15 Jahre hinweg Aufträge in Bezug auf sechs Regionalgesellschaften mit mehr als 300 Filialen erhalten, um neben der üblichen Überwachung zur Vorbeugung von Kundendiebstählen MitarbeiterInnen mit Kameras zu bespitzeln und Privates auszuspionieren. Das Unternehmen hatte bislang Vorwürfe, seine MitarbeiterInnen heimlich zu überwachen, immer bestritten.

Der Detektiv berichtete, eine Aldi-Führungskraft in Dornstadt habe vor drei Jahren von ihm verlangt, er solle über den Spinden in der Mitarbeiterumkleidekabine mobile Miniaturkameras installieren. Als er ablehnte, sei ihm gedroht worden, er werde „alle Überwachungsaufträge verlieren", wenn er der Aufforderung nicht nachkomme. „Ich hatte weiterhin den Auftrag, alle Auffälligkeiten zu melden. Also auch, wenn ein Mitarbeiter zu langsam arbeitete, ich von einem Verhältnis der Mitarbeiter untereinander erfahren habe oder ich andere Details aus dem Privatleben mitbekam, zum Beispiel im Hinblick auf die finanzielle Situation des Mitarbeiters." Er sei angehalten worden, Miniaturkameras in Zentrallagern einzubauen, also an Orten ohne Publikumsverkehr. Deren Installation und das Speichern der so erhaltenen Daten ist verboten, wenn nicht ausdrücklich auf die Überwachung hingewiesen wird. In der schweizer Filiale Kreuzlingen will er mobile Kameras über der Kasse eingebaut haben, in der Filiale Kumbach vier Kameras über den Kassen, eine im Büro. Auf der Rechnung steht „Sonderdienstleistung". Häufig habe er zu den üblichen Kamerasystemen zusätzlich Mini-Anlagen installiert. Wenn er Zweifel an dem Vorgehen geäußert habe, sei ihm gesagt worden, der Auftrag komme von ganz oben und „sei mit den Aldi-Rechtsanwälten abgeklärt". Der Detektiv beteuerte seine Angaben mit einer eidesstattlichen Versicherung. Rechnungen bis 5.000 Euro müssen bei Aldi-Süd von einem Mitarbeiter der Geschäftsführung abgezeichnet werden, ab 5.000 vom Geschäftsführer persönlich. Der Detektiv schickte mehrere Rechnungen mit Beträgen über 5.000, die bezahlt wurden, wobei aus einigen eindeutig hervorgehe, dass Mini-Kameras eingesetzt worden sind.

Im Frühjahr 2008 war Konkurrent Lidl in die Kritik geraten, weil er Mitarbeiter systematisch durch Kameras und Detektive überwachen ließ (DANA 3/2009, 109; Arnsperger, DANA 1/2011, 10 ff). Dieser Skandal löste in der Branche Vorsicht bei der Wahl der Überwachungsmethoden aus, nicht so aber anscheinend bei Aldi Süd. Aldi Süd wies die Vorwürfe zurück. Eine Überwachung von Mitarbeitern im Hinblick auf deren Arbeitsleistung sei in den Rahmenverträgen für Detektiveinsätze ausdrücklich ausgeschlossen. Es habe keine Anweisung gegeben, Auffälligkeiten wie private Details zu melden. Bei der Überwachung des Logistiklagers seien Mitarbeiter und Fahrer informiert worden, die Aufnahmen seien auf CDs gespeichert, ausgewertet und danach umgehend vernichtet worden. Illegale und nicht vertragskonforme Praktiken der Detektive würden nicht freigegeben und nicht geduldet. Abgezeichnete Rechnungen über 5.000 Euro „betreffen jedoch keine unseriösen Praktiken" (Amann, Tietz, Auftrag von ganz oben, Der Spiegel 2/2013, 69; Ex-Detektiv: Aldi Süd bespitzelt Mitarbeiter mit Kameras, www.focus.de 06.01.2013; siehe auch DANA 2/2012, 76 ff.).

Sachsen

Datenlecks und Ermittlungen bei Unister

Die sächsische Generalstaatsanwaltschaft hat ihre Ermittlungen gegen den Online-Reiseverkäufer Unister, der u. a. Fluege.de oder Ab-in-den-Urlaub.de anbietet, ausgeweitet. Gemäß Behördensprecher Wolfgang Klein wird jetzt auch wegen des Verdachts des illegalen Adresshandels und wegen gefälschter Preisangaben ermittelt. Seit längerem stand Unister im Verdacht, illegal Versicherungen verkauft und dabei Steuern in Millionenhöhe hinterzogen zu haben. Am 30.01.2013 wurden erneut umfangreiche Durchsuchungen bei Unister und deren Geschäftspartnern durchgeführt. 40 Polizeibeamte und vier Staatsanwälte waren in der Zentrale in Leipzig sowie in Potsdam und Bayern im Einsatz. Unister bestätigte dies und sprach von „Nachuntersuchungen in den Räumen von Unister". Man habe weitere Unterlagen an die Behörden übergeben und sei an Aufklärung interessiert. Unister gab zudem bekannt, mit dem Betriebswirt Frank Hillmer einen neuen Datenschutzbeauftragten berufen und damit eine Forderung des sächsischen Datenschutzbeauftragten erfüllt zu haben, der die Standards in der Firma kritisiert hatte.

Staatsanwalt Klein erläuterte: „Es besteht der Verdacht, dass über mehrere Jahre Kundendaten ohne Wissen der Betroffenen verkauft worden sind an kommerzielle Adresshändler." Damit habe Unister mehrere Millionen Euro gemacht. Die Ermittlungen wegen illegalen Adresshandels seien durch eine Strafanzeige des sächsischen Datenschutzbeauftragten ins Rollen gebracht worden. Unister erklärte dazu: „Über diese Anschuldigung sind wir nicht nur überrascht, sondern sie entbehrt jeder Grundlage. Diese Unterstellung ist eine echte Unverschämtheit."

Die Generalstaatsanwaltschaft glaubt zudem, dass Unister mit gefälschten Preisen auf seinen Reiseseiten gegen das Gesetz gegen unlauteren Wettbewerb verstoßen hat. Systematisch seien den KundInnen auf den Reiseportalen Schnäppchen vorgegaukelt worden durch sogenannte Streichpreise, die allerdings frei erfunden waren. Die Streichpreise, angebliche Ursprungspreise für Reisen oder Flüge, seien niemals wirklich verlangt worden, erläuterte Klein. „Man hat auf breiter Front etwas vorgetäuscht, was nicht da war." Dazu sei ein ausgefeiltes, hoch professionelles

Computerprogramm eingesetzt worden, das die Schnäppchenpreise erzeugt habe. „Wir haben den Algorithmus gefunden.“ Auch diese Vorwürfe wies Unister in einer Stellungnahme zurück.

Gegen die Leipziger Internetfirma Unister gab es erst im Dezember 2012 den Vorwurf, auf Grund von Sicherheitslücken seien KundInnen geschädigt worden, die mit ihrer Kreditkarte gezahlt haben. 400.000 Kundendaten sollen nicht ausreichend geschützt worden sein. Dadurch sei ein Schaden von rund einer Million Dollar entstanden. Als Konsequenz habe Unister umgerechnet rund 140.000 Euro Straf- und Wiedergutmachungszahlungen an die Kreditkartenkonzerne Visa und Mastercard entrichtet. Das Unternehmen erklärte in einer Stellungnahme, die Datensicherheit bei den eigenen Portalen sei durchaus gewährleistet. Seit Februar 2012 sei das Sicherheitskonzept sogar mit dem sogenannten Payment Card Industry Data Security Standard (PCI DSS) zertifiziert. Dieser gehöre zu den schärfsten Sicherheitsvorschriften im elektronischen Banken- und Zahlungsverkehr weltweit. Andreas Schneider vom Sächsischen Datenschutzbeauftragten sagte dagegen, das Unternehmen habe für eine wirksame Datenschutzkontrolle bislang „keine qualifizierten Unterlagen vorlegen können“. Die Presse berichtete schon im Dezember 2009 und 2011 von Sicherheitslücken. Möglicherweise wurden diese Daten an Kreditkartenbetrüger weitergegeben. Anfang 2013 wurde erneut berichtet, dass Namen und Flugrouten von 4.700 Flugreisenden von Ryanair für andere KundInnen einsehbar gewesen seien. Die Staatsanwaltschaft Leipzig ermittelt zudem wegen Ungereimtheiten bei der Dating-Plattform partnersuche.de. Dort sollen in den vergangenen zwei Jahren mit erfundenen Profilen Kontaktanfragen vorgetäuscht und so KundInnen in Abonnements gelockt worden sein.

Die neuen Verdachtsmomente richten sich gegen jene acht Unister-Führungskräfte, gegen die bereits wegen Steuerbetrugs ermittelt wird. Drei Manager hatten zwischenzeitlich in Untersuchungshaft gesessen, die Haftbefehle wurden jedoch gegen Zahlung von Kautionen und Meldeauflagen außer Vollzug gesetzt. Der Unister-Gründer Thomas Wagner hatte angekündigt, sich von der Spitze des Unternehmens zurückzuziehen. Angeblich läuft die Suche nach einem Nachfolger. Das Unternehmen, das auch Seiten wie geld.de und auto.de betreibt, beschäftigt nach eigenen Angaben 1.900 Mitarbeitende. Angaben zu Umsatz und Gewinn macht Unister nicht. In aktuellen Stellenanzeigen spricht das Unternehmen jedoch davon, einen „Jahresumsatz im zehnstelligen Eurobereich“ zu machen, also von Milliarden (Datenleck bei Unister verursacht Millionenschaden, www.focus.de 19.12.2012; Erneut Datenleck bei Unister, SZ 05./06.2013, 23; Online-Händler Unister beruft neuen Datenschutzbeauftragten, www.finanznachrichten.de 29.01.2013; Unister soll Adressen seiner Kunden verhökert haben, www.welt.de 30.01.2013)

Sachsen

Kfz-Kennzeichen-Scanner im anlasslosen Einsatz

Die Polizei im Freistaat Sachsen setzt sechs Kameras ein, die Autokennzeichen überwachen und gestohlene Autos schnell erfassen sollen. Das System CatchKen erkennt die Kennzeichen vorbeifahrender Fahrzeuge und vergleicht sie mit einer Datenbank, einer Kfz-Fahndungsliste. Das Catch Ken System wurde mit der holländischen Polizei für die polizeitechnischen Zwecke von Kennzeichenlese-Verfahren bereits in den 90er-Jahren entwickelt. Wird eine Übereinstimmung mit einem Kennzeichen der Datenbank ermittelt, erfolgt eine optische und akustische Alarmierung der Messbeamten. Die Polizei soll das gesuchte Fahrzeug dann verfolgen und anhalten. Gibt es keinen Treffer, werden die erfassten Daten gelöscht. Auf die Fahndungsliste gelangen gestohlene Kfz, aber auch, wenn Kfz aus anderen Gründen gesucht werden. Innenminister Markus Ulbig (CDU) stellte das sogenannte automatisierte Kennzeichenerkennungssystem vor: „Im Kampf gegen Autoschieber ist das ein weiterer Baustein. Die Voraussetzung, dass ein Treffer angezeigt wird, ist, dass ein Auto als gestohlen gemeldet wurde.“

Gemäß einer Antwort auf eine Kleine Anfrage der Grünen-Fraktion im Landtag sind für das Projekt rund 150.000 Euro vorgesehen. Autodiebe sollen das vorrangige Ziel der Ermittler sein, die mit der auf einem Dreibein montierten Kamera und angeschlossenem Computer künftig ähnlich wie bei Geschwindigkeitskontrollen unterwegs sind. Wird ein gestohlener Wagen erfasst, bevor er im Fahndungssystem registriert ist oder nachdem das Kennzeichen ausgetauscht wurde, bleibt er unerkannt. Laut Regierungsantwort hatte die Polizei in einer Testphase mehr als 18.000 Kennzeichen erfasst, ohne dass Autodiebe gefasst wurden. Gestoppt wurden zwei Fahrer, die ihr Fahrzeug nicht versichert hatten – was auch eine Straftat darstellt. Ulbig: „Es gibt keine Grenzen bezogen auf die Deliktarten.“ Auch andere Straftäter sollen auf diese Weise selbst aus dem dichtesten Verkehr gezogen werden, wenn ihr Fahrzeug zur Fahndung ausgeschrieben ist (Big Brother auf sächsischen Autobahnen, www.welt.de 04.12.2012).

Sachsen-Anhalt

Polizeirechtsentwurf beeinträchtigt kommunikative und informationelle Grundrechte

Der Landtag Sachsen-Anhalt berät über einen Gesetzentwurf der schwarzroten Regierung zur Novellierung des Polizeirechts. Der Vorstoß zur „Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung“ sieht umfangreiche neue Befugnisse für die Strafverfolger vor. So sollen sie etwa den Mobilfunk abschalten und Staatstrojaner zum Abhören von Internet-Telefonaten einsetzen dürfen.

Im geplanten neuen § 33 des Entwurfs heißt es: „Die Polizei kann von jedem Diensteanbieter verlangen, Kommunikationsverbindungen zu unterbrechen oder zu verhindern.“ Voraussetzung soll eine unvermeidliche „Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder ei-

nes Landes oder für Leib, Leben oder Freiheit einer Person" sein. Der Eingriff sei „unverzüglich herbeizuführen und für die Dauer der Anordnung aufrechtzuerhalten". Der Polizei soll es zudem gestattet sein, selbst zu diesem Zweck „technische Mittel einzusetzen".

„Örtlichen Bereich, Zeit und Umfang der Maßnahmen ordnet der Behördenleiter oder ein von ihm Beauftragter an." In der Begründung heißt es, die Unterbrechung oder Verhinderung von Telekommunikation greife „nicht in den Artikel 10 ein, so dass ein Richtervorbehalt grundsätzlich nicht notwendig ist". Erst im Nachhinein soll die Polizei „unverzüglich eine richterliche Bestätigung" einholen müssen, wenn die Blockade länger als zwei Tage fortgeführt werden soll. Bisher ist der Einsatz entsprechender „Jammer" etwa zum Unterbrechen des Mobilfunks trotz schwerer Bedenken der Netzbetreiber in manchen Bundesländern in Justizvollzugsanstalten erlaubt. Der großen Koalition in Sachsen-Anhalt geht es laut Begründung vor allem um das Verhindern von Sprengstoffanschlägen. Landesinnenminister Holger Stahlknecht nannte als Beispiele „Bomben, die per Handy ausgelöst werden, Amokläufe oder Geiselnahmen" und ergänzte: „Es ist nicht unsere Intention, den Handyempfang bei Demonstrationen zu stören."

Weit gefasst sind auch die vorgesehenen Kompetenzen zum Erheben von Telekommunikationsinhalten und deren Begleitumstände wie Verbindungs- oder Standortdaten. Der Einsatz entsprechender Mittel soll präventiv zur Gefahrenabwehr möglich sein. Außer bei Gefahr in Verzug ist hier eine Richtergenehmigung einzuholen. § 17b bezieht sich auf die sogenannte Quellen-Telekommunikationsüberwachung, also das heimliche Eindringen in ein informationstechnisches System, um auch gegebenenfalls verschlüsselte Internet-Telefonie abhören zu können. An dem Rechner oder IT-Gerät sollen dabei nur Veränderungen vorgenommen werden, „die für die Datenerhebung unerlässlich sind". Eingeschränkt wird die Erlaubnis auf Inhalte eines laufenden Telekommunikationsvorgangs. Experten warnen seit Langem, dass nach Installation eines Abhörtrojaners die Grenzen zu einer umfassenderen Online-Durchsuchung eines Systems fließend sind.

Die Initiative sieht sowohl beim Belauschen der Telekommunikation als auch bei der gleich mit angepackten Reform des Großen Lauschangriffs den Schutz des Kernbereichs der privaten Lebensgestaltung vor. Daten dürfen demnach durch Observation oder den Einsatz technischer Mittel von vornherein nur erhoben werden, soweit nicht aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass die Überwachung Informationen aus der an sich absolut geschützten Intimsphäre betrifft. Trotzdem bestehen bleiben soll aber, so die Begründung, zugleich die Befugnis, „die Daten weiterhin aufzuzeichnen und automatisiert zu speichern". Dies sei etwa nötig, wenn eine Unterredung in einer fremden Sprache erfolge. Den Kernbereich berührende Inhalte müssten dann nach einer Prüfung im Nachhinein gelöscht werden.

Das schon im Sommer vorgelegte Papier sieht eine Reihe weiterer Befugnisse vor, etwa zum Orten von suizidgefährdeten oder hilflosen Personen mithilfe eines IMSI-Catchers, zum Anfertigen von Videoaufzeichnungen zur Eigensicherung von Vollzugsbeamten „bei Anhalte- und Kontrollsituationen" oder zum Anordnen von DNA-Analysen zur Identifizierung von hilflosen Personen und Toten. Ende November 2012 fand zu dem Entwurf eine Anhörung im Landtag statt. Besonders umstritten war dabei der ebenfalls vorgesehene polizeiliche AIDS-Zwangstest „zur Abwehr einer Infektionsgefahr".

Bereits im Vorfeld forderte der Landesdatenschutzbeauftragte Harald von Bose, unter anderem die Bestimmungen zur präventiven Telekommunikationsüberwachung oder zur Rasterfahndung aus dem Entwurf zu streichen. Verbände der Polizeigewerkschaften begrüßten das Vorhaben dagegen prinzipiell und plädierten an einigen Stellen für Ausweitungen. Die Gewerkschaft der Polizei (GdP) etwa sprach sich dafür aus, die neuen Kompetenzen zum Durchführen verdeckter Datenerhebungen in Wohnräumen oder im Internet auch ausdrücklich allgemein zur „Verhütung schwerwiegender Straftaten" vorzusehen. Auch würde eine Vielzahl von Fallbeispielen aus der polizeilichen Praxis die Erforderlichkeit einer prinzipiellen polizeilichen Befugnis für heimliche Online-Durchsuchungen belegen.

Der grüne Landtagsabgeordnete Sebastian Striegel sah bei der Debatte kurz vor Weihnachten 2012 durch den Entwurf „Bürgerrechte in sehr massivem Umfang gefährdet". Die linke Abgeordnete Henriette Quade hielt das Gesetz für „viel zu weit gefasst und damit verfassungswidrig". Für den SPD-Fraktionsvize Rüdiger Erben war diese Kritik an den Neuregelungen „böswillig überzogen". Die Koalition reagiere auf Gefahren, die bei Verabschiedung des bisherigen Polizeigesetzes noch nicht denkbar waren: „Damals gab es halt noch keine Handys" (Krempl www.heise.de 03.12.2012; Bielicki, Polizei soll Mobilfunk abschalten können, u. Prantl, Wie ein Grundrecht eine Rübe wird, SZ 18.12.2012, 1, 4).

Thüringen

Datenschutzbeauftragter kritisiert Telefon-Mithörfunktionen

Nach Mitteilung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Lutz Hasse verfügen die Telefonanlagen in der Thüringer Polizei und des Innenministeriums über fragwürdige Funktionen. Die sog. Aufschaltfunktion ermöglicht es, geführte Telefonate von Dritten mitzuhören; mit der sog. Babyfonfunktion können trotz aufgelegtem Telefonhörer die Gespräche in demjenigen Raum, in dem sich der Telefonapparat befindet, mitgehört werden. Das Thüringer Innenministerium habe dies bestätigt.

Ohne eigene Kenntnis und ohne Möglichkeit der eigenen Einflussnahme könnten Aufschalt- und Babyfonfunktionen aktiviert werden. Bei diesen Funktionen handele es sich um den „marktüblichen" Standard von Telefonanlagen. Hasse befürchtet, dass sich diese Funktionen nicht auf die Telefonanlagen der Thüringer Polizei oder des Thüringer Innenministeriums beschränken und auf die gesamte Landesverwaltung und die

Kommunalverwaltungen erstrecken. Nicht unwahrscheinlich sei auch, dass Telefonanlagen in vielen Unternehmen innerhalb und außerhalb von Thüringen über derartige Funktionen verfügen. Hasse forderte und kündigte für seinen Zuständigkeitsbereich an, dass die technischen und rechtlichen Sicherungsmechanismen kontrolliert und im Fall von Mängeln eingeführt werden müssten, um das offene Tor des Missbrauchs möglichst dicht zu schließen. Das gelte auch für (Fern-)Wartungsarbeiten. Personal- und Betriebsräte sollten entsprechende Vereinbarungen mit dem Dienstherren bzw. den Arbeitgebern treffen. Der TLfDI bat die Bürgerinnen und Bürger um Mithilfe bei der Aufklärung dieser prekären Situation (TLfDI PM v. 14.01.2013, Big Brother - Standard).

Datenschutznachrichten aus dem Ausland

Europa

Polizei erhält Zugriff auf Eurodac

Wer in der Europäischen Union (EU) Asyl beantragt, muss schon seit Langem zur Durchführung der Verfahren Fingerabdrücke abgeben, die in der europaweiten Datenbank Eurodac gespeichert werden. Gespeichert werden dort auch die Abdrücke der Menschen, die bei illegaler Einreise oder Aufenthalt in der EU aufgegriffen werden. Nach Plänen der EU-Kommission soll die Polizei im Rahmen ihrer Ermittlungen bei Verdacht auf schwere oder terroristische Straftaten diese Dateien abfragen können. Der Innenausschuss des EU-Parlaments billigte den Regelungsvorschlag am 18.12.2012 mit großer Mehrheit der Sozialdemokraten, Liberalen und Konservativen. Die Forderung von einigen Sozialdemokraten, der Grünen und der Linken, alle Passagen zum Polizeizugriff auf die Fingerabdrucks-Datei zu streichen, fand wegen der Verweigerung der Liberalen keine Mehrheit. Die Grünen sprachen von einem „Desaster für den Datenschutz und für die Rechte der Flüchtlinge“.

Hilfsorganisationen klagen immer wieder darüber, dass Flüchtlinge wie Kriminelle behandelt werden und z. B. in Abschiebehaft genommen werden - ungeachtet der Tatsache, dass das Asylrecht zu den Grund- und Menschenrechten zählt. Die Kritik erhält mit dem polizeilichen Datenzugriff neue Nahrung. In Eurodac werden seit 2003 die Fingerabdrücke von allen über 14 Jahre alten Flüchtlingen für 10 Jahre verwahrt. Rechtsgrundlage ist die Eurodac-Verordnung aus dem Jahr 2000 „zur effektiven Anwendung des Dubliner Abkommens“. Wegen der Kritik an der Einrichtung dieser Datei war deren Zweck und Datenverarbeitung zunächst eng gefasst: Die Fingerabdruck-Datei sollte einzig und allein dafür da sein, die Zuständigkeit für das Asylverfahren zu regeln. Die sogenannte Dublin-II-Verordnung legt fest, dass allein der EU-Staat für das Asylverfahren zuständig ist, den der Flüchtling auf seiner Flucht als erstes betritt. Um das durchzusetzen und zu verhindern, dass ein Flüchtling gleichzeitig oder nacheinander mehrere Asylverfahren in verschiedenen Ländern betreibt, wurde Eurodac eingerichtet.

Schon vor drei Jahren hatte die Kommission den Zugriff der Sicherheitsbehörden auf Eurodac betrieben, diesen Vorschlag aber nach Kritik aus dem Europa-Parlament wieder zurückgezogen. Dass der Kommissions-Vorschlag wieder vorangetrieben wird, hat damit zu tun, dass auch über gemeinsame EU-Standards für die Asylverfahren und für die Aufnahme von Flüchtlingen verhandelt wird. Offenbar soll die Zustimmung der EU-Mitgliedsländer zu kleinen Verbesserungen bei diesen Standards damit erkauft werden, dass die nationalen Sicherheitsbehörden den Zugriff auf Eurodac erhalten. Peter Hustinx, der Europäische Datenschutzbeauftragte, kritisierte das Vorhaben. Er warnte vor einem „Risiko der Stigmatisierung“ und einer schleichenden Erosion der Grundrechte. Die enge Zweckbindung der Datei wird aufgehoben, die Polizei soll umfassenden Zugriff auf die Fingerabdrücke erhalten. Nach den derzeitigen Formulierungen soll der Zugriff zur Verfolgung schwerer Straftaten und zur Terrorbekämpfung erlaubt werden, um z. B. Fingerabdrücke von einem Tatort mit den Eurodac-Fingerabdrücken der Flüchtlinge zu vergleichen; zuvor muss die Polizei aber ihre eigenen Datenbanken und die anderer Mitgliedsländer befragen.

Die EU-Kommission bereitet nach Presseinformationen eine weitere Verordnung vor, wonach nicht nur von Flüchtlingen, sondern von sämtlichen EU-Ausländern Fingerabdrücke genommen und gespeichert werden sollen. Alle Menschen, die von außerhalb der EU kommen, sollen sich bei der Ein- und Ausreise über EU-Grenzen mit Fingerabdrücken registrieren müssen; Strafverfolgungsbehörden sollen auf diese Datenbank Zugriff erhalten. BürgerrechtlerInnen und DatenschützerInnen befürchten, dass eines Tages auch der Zugriff auf die Fingerabdrücke erlaubt werden wird, die auf den RFID-Chips der Reisepässe der EU-BürgerInnen gespeichert sind. Seit 2007 erhalten auch BundesbürgerInnen nur noch dann einen Reisepass, wenn sie in dem Dokument ihre Fingerabdrücke speichern lassen. Das Verwaltungsgericht Gelsenkirchen hat erhebliche Zweifel, ob den Menschen diese Prozedur zugemutet werden darf und legte diese Frage im Mai 2012 dem Europäischen Gerichtshofs (EuGH) zur Entscheidung vor. Der Kläger, ein Bochumer Rechtsanwalt, kritisiert das Überwachungspotenzial, das mit den Fingerabdrücken geschaffen werde. Ähnliches befürchtet die niederländische Justiz, die ebenfalls diese Frage dem EuGH vorgelegt hat. In den

Niederlanden hatten sich BürgerInnen geweigert, sich Fingerabdrücke nehmen zu lassen. Als ihnen daraufhin keine Reisepässe ausgestellt wurden, zogen sie vor Gericht (Prantl, Polizei soll Zugriff auf Fingerabdrücke erhalten, SZ 17.12.2012, 5; Zugriff auf Asyl-Datenbank, SZ 19.12.2012, 6).

Europa/USA

EU-Studien warnen vor behördlicher US-Überwachung bei Cloud-Diensten

Ein Gutachten des „Centre D'Etudes sur les Conflits" und des „Centre for European Policy Studies", beide in Belgien, das vom EU-Parlament (EP) in Auftrag gegeben wurde, warnt davor, dass sich US-Behörden heimlich Zugriff auf die Daten europäischer NutzerInnen bei Cloud-Anbietern wie Google, Facebook oder Dropbox verschaffen. Die Abgeordneten des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des EP wollten wissen, ob mit der Zunahme von Cloud Computing ein Anstieg von Cyber-Kriminalität einhergehe und ob Handlungsbedarf besteht. Gemäß der Studie „Fighting Cyber Crime and Protecting Privacy in the Cloud" besteht Handlungsbedarf, aber weniger wegen erhöhter Kriminalität; viel dramatischer sei der Verlust über die Kontrolle der Daten, wenn diese auf den Servern von US-Anbietern liegen. US-Ermittler können demnach bei einem Gericht einen geheimen Beschluss beantragen und die ausländischen Nutzerinnen und Nutzer überwachen. Ko-Autor des Berichts ist Caspar Bowden, der zuvor für den Datenschutz bei Microsoft Europe arbeitete.

Die Sicherheitsgesetze zur Terrorabwehr, die nach dem 11.09.2001 eingeführt wurden, machten es möglich. Mit dem Patriot Act wurden Ermittlern umfassende Abhöraktionen erlaubt; das zunächst befristete Gesetz wurde später dauerhaft verlängert. Während zumindest über die Folgen dieses Gesetzes in der Europäischen Union (EU) öffentlich debattiert wurde, sei das bei dem Foreign Intelligence Surveillance Amendment Act (FISAA) von 2008 schon nicht mehr der Fall gewesen, der die Massenüberwachung von Menschen aus Europa ermöglicht. In der EU gebe es für die Möglichkeit der politischen Massenüberwachung überhaupt kein Bewusstsein, so die Autoren der Studie: Die USA würden überwachen, die EU sich nicht um den Schutz der Rechte ihrer Bürger kümmern.

Die Autoren empfehlen deshalb den ParlamentarierInnen, sich um Rechtssicherheit beim Cloud Computing zu kümmern. Ihnen wird nahegelegt, mit den USA in Verhandlungen zu treten, damit das Menschenrecht auf Privatsphäre auch für europäische StaatsbürgerInnen gelte. Es sollten deutliche Warnungen verpflichtend vorgenommen werden: Denn wenn Cloud-Daten von der EU in die USA überführt werden, würden diese dem dortigen Überwachungsapparat ausgesetzt, was allen Betroffenen mitgeteilt werden müsse. Bowden sieht im FISAA eine Freikarte für alle Aktivitäten, welche die Interessen der US-Außenpolitik fördern. Das Gesetz ermögliche die Überwachung von europäischen JournalistInnen, AktivistInnen und PolitikerInnen, die sich in irgendeiner Weise mit Angelegenheiten beschäftigen, in denen die USA ihre Finger im Spiel haben. Der FISAA erlaube den USA die massenhafte Überwachung demokratischer politischer Aktivitäten und könne so weit gehen, dass man US-Cloud-Betreiber wie Google auferlegt, eine "live"-Übertragung von Daten europäischer Nutzenden zu schalten.

Eine weitere Studie von Rechtsexperten der Universität Amsterdam und dem niederländischen Institut für Informationsrecht mit dem Titel „Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act" kommt ebenso zu dem Ergebnis, dass die USA die unter dem Namen Patriot Act verabschiedeten Anti-Terror-Gesetze dazu nutzen können, Internet-Nutzende in Europa auszuspionieren. Das Gesetz erlaube umfassende Überwachungen von Telekommunikation und Internet, was auch Einfluss auf europäische Internet-Nutzende hat, etwa wenn sie auf so genannte Cloud-Dienste zurückgreifen. Ein Großteil der Anbieter von Cloud-Services hat seinen Sitz in den USA oder wickelt Geschäfte über die Vereinigten Staaten ab. Auch der FISAA erlaube der US-Regierung den Zugriff auf die Cloud-Daten. Die strengen Datenschutzrichtlinien der EU werden über diese Hintertür außer Kraft gesetzt.

Der US-Botschafter bei der EU, William Kennard, hatte erst im Jahr 2012 versucht, die Sorgen vor einer Totalüberwachung durch US-Behörden zu zerstreuen und zu relativieren. Es gebe rechtliche Vorkehrungen, um die Privatsphäre von Einzelpersonen zu schützen. Die Autoren der Studien konnte er damit nicht überzeugen. Sie verweisen unter anderem auf ein gigantisches Rechenzentrum, das derzeit vom US-Geheimdienst NSA errichtet wird. Auch den Vortrag eines ehemaligen NSA-Mitarbeiters, des Whistleblowers William Binney, auf der Hackerkonferenz „Hope" in New York im vergangenen Sommer führen sie an. Ende Dezember 2012 hatte Binney auf dem Kongress des Chaos Computer Clubs in Hamburg vor der US-Überwachung gewarnt.

Die Berichte wurden im Dezember 2012 vorgelegt und haben Relevanz im Zusammenhang mit der parallel diskutierten EU-Datenschutzreform. EU-Kommission und EU-Parlament verhandeln über eine umfassende Neuordnung des Datenschutzes in Europa. In der belgischen Studie geben die Forscher detailliert Hinweise zu aktuellen Regularien hinsichtlich des Datenschutzes und des grenzüberschreitenden Datenaustauschs. Die Forscher schlagen vor, bis zum Jahr 2020 wenigstens 50% der EU-Dienste auf Cloud-Computern unter die vollständige rechtliche Kontrolle der EU zu bekommen. Laut der EP-Abgeordneten Sophie in 't Veld könnten strengere Regelungen für die EU das Problem zwar nicht lösen, da die aktuellen Gesetze EU-Bürgerinnen und -Bürger nicht vor Anfragen aus dem Ausland schützen können. Das sei jedoch kein Grund, den Konflikt zu akzeptieren und keine Gegenmaßnahmen einzuleiten. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hatte zu der Fragestellung schon im November 2011 auf die rechtliche Problematik hingewiesen (Reißmann, EU-Studie warnt vor Überwachung durch die USA, www.spiegel.de 10.10.2013;

Bergert, US-Behörden könnten durch Patriot Act europäische Nutzer ausspionieren, www.pcwelt.de 07.12.2012; US-Spionagegesetz erlaubt den USA, europäische Bürger auszuschnüffeln, www.politaia.org 10.10.2013; ULD, https://www.datenschutzzentrum.de/internationales/20111115-patriot-act.html).

Europa/USA

Geheimbericht über US-SWIFT-Bankdatenzugriffe veröffentlicht

Die britische Bürgerrechtsorganisation Statewatch hat ein ursprünglich geheim gehaltenes Arbeitspapier der EU-Kommission veröffentlicht, in dem die Umsetzung des transatlantischen Abkommens zum Bankdatentransfer überprüft wird. Die USA haben demnach im Untersuchungszeitraum zwischen dem 01.02.2011 und dem 30.09.2012 monatlich durchschnittlich 1.590 Suchanfragen in Überweisungsinformationen durchgeführt, die über das Netzwerk der Society for Worldwide Interbank Financial Telecommunication (SWIFT) liefen. Insgesamt hätten Analysten des US-Finanzministeriums im Rahmen des „Terrorist Finance Tracking Program“ (TFTP) während der anderthalb Jahre 31.797 Mal auf die Daten zugegriffen. Dies sei im Durchschnitt deutlich weniger häufig gewesen als im Zeitraum des ersten Kontrollberichts, der von Anfang August 2010 bis Ende Januar 2011 reichte. Konkrete Angaben zu den abgefragten und durchsuchten Datenvolumina habe die US-Seite nicht gemacht.

Washington sehe diese Auskünfte als zentral für sein Terrorabwehrprogramm an, da damit detaillierte Hinweise auf die Herkunft der Überweisungsinformationen preisgegeben würden. Brüssel steht auf dem Standpunkt, dass zu diesem Punkt mehr Hinweise erforderlich seien, um die Reichweite des gesamten Projekts und dessen Auswirkungen auf die Bürgerrechte sowie dessen Verhältnismäßigkeit abzuschätzen. Erwähnt wird auch, dass das zuständige US-Ministerium von allen in die USA gereisten Prüfern der Kommission die Unterzeichnung einer Geheimhaltungserklärung verlangt habe, was aber deren Arbeit nicht behindert habe. Der Bericht unterstreicht, dass es sich nach Angaben Washingtons bei den untersuchten SWIFT-Daten um Zahlanweisungen von Finanzinstituten aus der ganzen Welt handelt. Der Großteil davon betreffe weder die Europäische Union (EU) noch deren Einwohner. Rein europäische Überweisungen, die den alten Kontinent nicht verlassen, blieben ohnehin außen vor. Über spezielle Anfragen der US-Behörde mit EU-Bezug muss gemäß der Übereinkunft Europol entscheiden. In der Evaluationsphase hat das europäische Polizeiamt dem Report nach 21 entsprechende Ersuche erhalten. In drei Fällen davon hätten die Europol-Beamten um zusätzliche Informationen gebeten. Letztlich sei aber keine US-Anfrage zurückgewiesen worden.

Die US-Seite wird mit dem Vermerk zitiert, dass die Genauigkeit Europols es erforderlich gemacht habe, den Umfang der im Rahmen eines Gesuchs mitgelieferten Unterlagen deutlich zu erhöhen. Habe man im August 2010 durchschnittlich 51 Seiten mitgeschickt, seien es im September 2012 schon 104 Seiten gewesen. Die Prüfer der Kommission erklärten zudem, dass sie es nicht als ihre Aufgabe angesehen hätten, sich über die Verfügungen der Polizeibehörde in Den Haag ein Urteil zu erlauben. Es sei eine bewusste Entscheidung gewesen, SpezialistInnen von Europol mit der Einschätzung der Anfragen zu betrauen und nicht etwa eine Datenschutzbehörde. Klar geworden sei ferner, dass die Überwachung der Prozesse durch einen ständigen EU-Beobachter in den USA gestärkt werden müsse. Dafür habe man inzwischen in Absprache mit der US-Regierung eine zweite Stelle geschaffen.

Gemäß dem Abkommen müssen nicht mehr für spezielle Untersuchungen benötigte Bankdaten nach fünf Jahren gelöscht werden. Das Prüfteam aus Brüssel zeigte sich nach eigenem Bekunden zufrieden damit, dass die US-Seite mit diesem Prozess begonnen habe. Da es sich dabei um eine „komplexe Übung“ handle, die sich auf das ganze System auswirke, sei ausgemacht worden, Informationen nicht laufend, sondern nach gewissen längeren Abständen zu vernichten. Gemäß dem Bericht sind zu dem Programm keine Auskunftswünsche von EU-BürgerInnen auf einem speziellen Anrufbeantworter beim Finanzministerium eingegangen. Fünf E-Mails von drei Personen habe man über die Adresse tftp@treasury.gov erhalten, die alle wunschgemäß hätten beantwortet werden können. Es habe keine Auskunftsbegehren von Betroffenen über vorgehaltene personenbezogene Daten gegeben, ebenso keine Wünsche zur Korrektur, zum Löschen oder Blockieren eigener Daten. Brüssel sieht insofern Verbesserungsbedarf, da diese verbrieften Rechte in der Öffentlichkeit kaum bekannt sind.

Gegenüber dem ersten Berichtszeitraum erhöhte sich nun die Zahl der Analysen, die europäische Einrichtungen und Mitgliedsstaaten von zuständigen US-Stellen angefordert hatten, von 10 auf 94. Ein Grund dafür sei, dass Europol für diese Möglichkeit der „Amtshilfe“ auf dem alten Kontinent geworben habe. Die US-Behörden hätten insgesamt erneut die Ansicht vertreten, dass das Programm zu großen Erfolgen im Kampf gegen den internationalen Terrorismus geführt habe. Ein Anhang listet dafür Beispiele auf. Die EU-Kommission hatte sich im Dezember 2012 anhand des Berichts erfreut gezeigt, dass alle Schutzvorschriften eingehalten würden. Der Bundesdatenschutzbeauftragte Peter Schaar sieht dagegen das wesentliche Problem ungelöst, dass es keine konkreten Anhaltspunkte über Ausmaß und Umfang der übermittelten Daten gebe (Krempl, Geheimbericht zum US-Zugriff auf Bankdaten im Netz, www.heise.de 03.01.2013).

Großbritannien

Staatliche Genkartierung

Die britische Gesundheitsbehörde NHS (National Health Service) will die DNA (Desoxyribonukleinsäure/DNS) von 100.000 Menschen kartieren lassen. Vor allem das Erbgut von KrebspatientInnen und Menschen mit seltenen Erkrankungen soll sequenziert und „anonymisiert“ gespeichert werden. Der britische Regierungschef David Cameron erläuterte: „Die Daten könnten

dabei helfen, komplexe Krankheiten besser zu verstehen, zu diagnostizieren und zu behandeln.“ Die umfangreichen genetischen Informationen böten die Chance, effektivere Medikamente zu entwickeln. Zudem sei es möglich, bereits existierende Therapieformen besser auf jede einzelne PatientIn abzustimmen. Am Erbgut ließe sich etwa erkennen, ob ein Mensch – zusätzlich zu seiner Krankheit – unter einer Stoffwechselstörung leidet. In diesem Fall könnte der Körper Chemotherapeutika schlechter verarbeiten und diese müssten geringer dosiert werden. Das Erbgut eines Menschen kann Hinweise darauf geben, welche Therapieform besonders gut zu ihm passt.

Die Regierung fördert das Programm mit umgerechnet rund 124 Millionen Euro. Im Jahr 2003 kostete eine vollständige Genkartierung noch rund 930 Millionen Euro. Seitdem sind die Kosten rasant gesunken. Nach Aussagen von Sir John Bell, Medizinprofessor an der Oxford University, kann in der nahen Zukunft eine Genkarte für nur 100 Pfund (= 124 Euro) erstellt werden. Dank der sinkenden Kosten sollen Genkartierungen im medizinischen Alltag eingesetzt werden. Großbritannien ist das erste Land, das diese nun in das staatliche Gesundheitssystem einführt. Bell: „Künftig wird jeder sein eigenes Erbgut sequenzieren lassen können.“ Die Bürgerrechtsorganisation Big Brother Watch sieht durch dieses Projekt die Privatsphäre der Menschen in Gefahr. Pharmafirmen könnten z. B. die Daten nutzen, um Medikamente gezielt an entsprechende Risikogruppen zu verkaufen. Werden die Daten nicht streng gesichert, könnten sie eines Tages noch viel mehr Informationen preisgeben (Klöckner, 100.000 Engländer lassen sich ins Erbgut gucken, www.zeit.de 11.12.2012).

Schweden

Randale nach Cybermobbing

Am 15.12.2012 war auf „Instagram“, einem zu Facebook gehörenden Internetportal, über das Fotos veröffentlicht werden können, ein Konto für „Huren und Schlampen“ eröffnet worden, auf dem Bilder von oft nackten oder halbnackten Schülerinnen aus der Hafenstadt Göteborg mit Namensangabe eingestellt wurden, verbunden mit der Aufforderung, mehr solche Fotos einzuschicken. Kommentare waren z. B.: „Sie läuft nur noch mit gespreizten Beinen durch die Stadt.“ Oder: „Das ist eine Albanerin, sie schläft mit dem Freund ihrer schwangeren Schwester.“ Die Anonymität der Einsender werde gewahrt. Als das Konto am 17.12. geschlossen wurde, enthielt es 200 solche Bilder, und war von fast 10.000 Leuten gesehen worden. Verschwunden waren die Bilder nicht, sondern längst vervielfältigt und über andere Konten auf Instagram und Facebook zugänglich. Gleichzeitig entstanden in mehreren Städten Schwedens ähnliche Internetkonten. Eine 17-Jährige vom „Framtidsgymnasiet“ wurde als Urheberin des ursprünglichen Kontos genannt.

Am Tag nach der Schließung des Kontos kam es im Zentrum von Göteborg zur Randale. Über Facebook wurde in der Nacht zuvor der Aufruf verbreitet, sich um 11 Uhr vor dem „Plusgymnasium“ zu versammeln, um die 17-jährige Mitschülerin fertigzumachen. Auf Bitten der Schulleitungen war die Polizei in mehreren Mannschaftsbussen angerückt. Dies half aber wenig gegen ca. 500 SchülerInnen, die die Polizei mit Flaschen, Steinen und Schneebällen bewarfen, Straßenlaternen zerstörten und auf Autos sprangen. Mehrere Jugendliche wurden von ihresgleichen niedergeschlagen. Viele SchülerInnen randalierten danach weiter in einem naheliegenden Einkaufszentrum, in dem Läden geschlossen werden mussten. Über Stunden war die Polizei nicht Herrin der Lage trotz Einsatzes von berittenen Beamten, Hunden und einem Hubschrauber.

27 SchülerInnen wurden in Gewahrsam genommen – einschließlich der 17-jährigen, die „fertiggemacht“ werden sollte. Sie wurde an einen geheimen Ort gebracht, wo sie unter Personenschutz gestellt wurde. Gegenüber der Polizei bestritt sie, etwas mit der Einrichtung des Kontos zu tun gehabt zu haben und erklärte, selbst darin abgebildet worden zu sein. Am Eingang des „Framtidsgymnasiet“ wurde ein Schild aufgehängt: „Die Schule ist geschlossen. Willkommen zurück am 7. Januar“. Das „Plusgymnasium“ wurde am 20.12. unter Aufsicht von „Dialogpolizisten“ wieder geöffnet. In den beiden vorangegangenen Tagen nahm die Polizei fast 60 Anzeigen wegen Verletzung der Persönlichkeitsrechte entgegen. Es gab auch weitere Unruhen, als etwa 200 SchülerInnen randalierend durch die Innenstadt Göteborgs zogen (Steinfeld, „Huren und Schlampen“, SZ 20.12.2012, 9).

Spanien

Katalanische Abhöraffäre erschüttert Politik

Eine Abhöraffäre von noch nicht absehbarem Ausmaß erschüttert die spanische Politik. Privatdetektive sollen in der Region Katalonien PolitikerInnen mehrerer Parteien, UnternehmerInnen und Prominente abgehört und ausspioniert haben. Die Detekteien haben, so Presseberichte, im Auftrag verschiedener Kunden mehr als 500 Dossiers angelegt. Von einem „katalanischen Watergate“ ist die Rede. Spaniens Innenminister Jorge Fernández Díaz bestätigte, dass die Polizei Ermittlungen eingeleitet hat. Die Affäre wurde öffentlich, nachdem die Chefin der konservativen Volkspartei in Katalonien (PPC), Alicia Sánchez-Camacho, bei einer Unterredung in einem Restaurant abgehört worden war und Anzeige erstattet hatte. Journalisten äußerten den Verdacht, die Sozialisten (PSC) hätten die Abhöraktion in Auftrag gegeben. Der PSC-Parteichef Pere Navarro bestätigte, dass seine Partei Aufträge an Detektivbüros erteilt habe. Dabei sei es aber nur um Sicherheitsfragen gegangen und nicht um Abhöraktionen.

Ein früherer Polizist, der bis vor kurzem für ein großes Detektivbüro gearbeitet hatte, soll nach Presseinformationen den Sicherheitsbehörden umfangreiches Material aus den Dateien der Agentur zur Verfügung gestellt haben. Danach sollen Politiker aller Parteien sowie Firmenchefs, Richter und Staatsanwälte observiert worden sein. Der Sprecher der Regionalregierung von Katalonien, Francesc Homs, äußerte in Barcelona den Verdacht, die Affäre sei ans Licht

gebracht worden, um die angestrebte Schaffung eines unabhängigen katalanischen Staates zu sabotieren. „Warum hat man den Skandal nicht schon vor zwei Jahren aufgedeckt?“ Katalonien wird von dem Bündnis CiU Convergència i Unió (Konvergenz und Union) regiert. Es besteht aus einer liberalen und einer christdemokratischen Partei. Die Affäre schädigt weiter das Ansehen der Politik bei der spanischen Bevölkerung, das durch Korruptionsvorwürfe und die katastrophale Wirtschafts- und Finanzsituation leidet (www.spiegel.de, Katalonien: Abhöraffäre erschüttert Spanien, 15.02.2013; Abhöraffäre in Spanien, SZ 16./17.02.2013, 8).

USA

Behördenauskünfte durch Google nehmen weiter zu

US-Behörden forderten im globalen Vergleich am häufigsten Nutzerdaten von Google an. Das geht aus den aktuellen Zahlen zum Halbjahr Juli bis Dezember 2012 hervor, die der Suchmaschinenkonzern am 23.01.2013 in seinem Transparenzbericht veröffentlicht hat. Demnach kamen 8.438 Anfragen zu 14.791 Nutzerkonten aus den Vereinigten Staaten (USA) – über ein Drittel der weltweit 21.389 Anfragen zu 33.634 Konten in diesem Zeitraum. Bei 88% der US-Anfragen stellte Google auch die Daten bereit. Auf dem 2. Platz folgt Indien mit 2.431 Anfragen zu 4.106 Nutzerkonten, danach Frankreich mit 1.693 Ersuchen zu 2.063 Konten. Deutschland liegt in der Halbjahres-Rangliste auf Platz 4 mit 1.550 Anfragen zu 1.944 Konten, wovon bei 42% der Behördenersuchen Auskünfte gegeben wurden.

Im Gesamtjahr 2012 wurden 42.327 Anfragen weltweit gestellt, im Vorjahr waren es noch 34.001. Auch aufs ganze Jahr gesehen stehen die USA mit 16.407 Anfragen an der Spitze, ein Anstieg um rund ein Drittel gegenüber den 12.271 US-Ersuchen von 2011. Deutsche Behörden hakten 2012 insgesamt 3.083 Mal bei Google nach, 2011 lag die Anfragenzahl hierzulande noch bei 2.491. Erstmals schlüsselt Google in seinem Bericht auch für die USA auf, welchen juristischen Hintergrund die Anfragen haben. 68% der Auskunftsersuchen gründeten sich auf behördliche Anordnungen, die laut Google am einfachsten zu bekommen sind, weil sie keinen richterlichen Erlass benötigen. Bei 22% handelte es sich um richterliche Durchsuchungsbefehle, bei 10% um sonstige Gerichtsanordnungen.

Google teilte mit, dass man von nun an von US-Behörden Durchsuchungsbefehle für die Anforderung von Clouddaten fordert. Zuletzt stand Google unter Kritik, da zwei Drittel der weitergegebenen Nutzerdaten ohne Durchsuchungsbefehl ausgehändigt wurden. Der Electronic Communications Privacy Act ermöglicht US-Behörden den Zugriff auf derartige Daten ohne Durchsuchungsbefehl, wenn sie sich bereits länger als 180 Tage auf den Servern von Google befinden. Google schränkt dieses Privileg nun eigenmächtig ein. Der Google-Sprecher Chris Gaither erklärte, dass man sich auf den vierten Verfassungszusatz berufe, der unrechtmäßige Durchsuchungen verbietet. Eine gerichtliche Auseinandersetzung möchten die US-Behörden offenbar vermeiden, da das 1986 verabschiedete Gesetz bereits mehrmals vor Gericht unter Beschuss geraten ist.

Anders als in den vorherigen Berichten macht der Konzern diesmal keine Angaben zur Zahl der Löschanfragen von Behörden. Diese sollen künftig separat mitgeteilt werden. Google hatte seinen globalen Transparenzbericht erstmals 2010 veröffentlicht und bringt seitdem eine regelmäßige Aktualisierung im Halbjahres-Rhythmus (vgl. DANA 4/2012, 175). Im Juni vergangenen Jahres hatte das Unternehmen eine erhebliche Zunahme staatlicher Löschanfragen beklagt (USA fragten am häufigsten Nutzerdaten von Google ab, www.heise.de 23.01.2013; Google verschärft Regeln für US-Behörden, futurezone.at 24.01.2013; https://www.google.com/transparencyreport/).

USA

Nacktscanner an Flughäfen werden abgebaut

Die Transportation Security Administration (TSA) baut ihre Nacktscanner an den Sicherheitskontrollen ab. Die US-Bundesbehörde, die u. a. für die Sicherheit an Flughäfen verantwortlich ist, hat noch 174 dieser Geräte an knapp 30 Airports im Einsatz. Sie sollen bis Ende Mai 2013 komplett durch Scanner ersetzt werden, die mit aktiver Millimeterwellentechnologie arbeiten. Anders als bei den alten Nacktscannern zeigen die neuen Kontrollen keine realistischen Körperbilder an, sondern markieren lediglich verdächtige Objekte an einem menschlichen Piktogramm. In Deutschland sind die Scanner bereits am Frankfurter Flughafen im Betrieb (DANA 4/2012, 172 f.).

Die TSA reagiert mit dem Abbau auf ein jüngst vom US-Kongress verabschiedetes Gesetz, das detaillierte Ganzkörperaufnahmen bei den Passagierkontrollen verbietet. KritikerInnen sahen in der Nacktscanner-Untersuchung einen Eingriff in die Privatsphäre der Fluggäste. Marc Rosenberg von der US-Bürgerrechtsorganisation Electronic Privacy Information Center meinte: „Es ist ein gutes Ergebnis, wenn TSA-Beamte zukünftig nicht in dunklen Räumen sitzen und sich Nacktbilder von Fluggästen anschauen.“ Die nun eingeleiteten Maßnahmen der TSA würden ihre größten Bedenken hinsichtlich der Sicherheitskontrollen zerstreuen.

Seit 2007 wurden die Nacktscanner auf US-Flughäfen eingesetzt. Der Gebrauch ist im Prinzip freiwillig; wer so nicht auf gefährliche Gegenstände hin überprüft werden will, muss ein intensives Abtasten per Hand über sich ergehen lassen. Statt nur leicht über die Kleidung zu streifen, wird „vorschriftsmäßig“ mit festem Druck über den ganzen Körper gewischt, was manche Passagiere als „Grapschen per Gesetz“ empfinden. Die Empörung richtet sich nicht nur gegen diese Verletzungen der Intimsphäre, sei es beim Durchleuchten oder beim Abtasten. An den alten Geräten war auch die Strahlenbelastung kritisiert worden. Hiermit habe, so die TSA, der Wechsel aber nichts zu tun. In der EU ist der Einsatz von Röntgenscannern an Flughäfen verboten. Die alten Nacktscanner werden allerdings nicht verschrottet. Für die Geräte sollen neue Standorte gefunden werden - unter anderem in US-Botschaften, beim Militär und in Gefängnissen (US-Flughäfen verzichten auf Nacktscanner, www.spie-

gel.de/reise/ 24.01.2013; US-Flughäfen schaffen Ganzkörper-Scanner ab, SZ 21.01.2013, 8; Nacktscanner von US-Flughäfen verbannt, www.sueddeutsche.de 21.01.2013).

USA

Zeitung veröffentlicht Namen und Adressen von Waffenbesitzenden

Mehr als 33.000 BürgerInnen des US-Bundesstaates New York erlebten am Heiligabend 2012 eine Überraschung: Die Lokalzeitung „The Journal News" hatte ihre Namen und Adressen in einer interaktiven Landkarte der Bezirke Westchester und Rockland unter der Überschrift veröffentlicht: „Wo sind die Waffenscheine in deiner Nachbarschaft?" Die lapidare Begründung der Zeitung für die Ermöglichung der Identifizierung der Waffenbesitzer: „Die Bürger interessieren sich dafür." Zum Beweis wurde ein anonymer Nachbar eines Mannes angeführt, der im Mai eine Frau auf der Straße angeschossen hatte. Der Nachbar sagte dem Blatt, wenn er von dem Waffenarsenal in der Nachbarschaft gewusst hätte, wäre er an einen anderen Ort gezogen. Nach dem Amoklauf von Newtown am 14.12.2012 mit 27 Todesopfern diskutiert ganz Amerika über den Umgang mit Schusswaffen. Auch die LeserInnen von The Journal News hatten lebhaft über strengere Waffengesetze debattiert. Das Blatt gehört zum Verlag „Gannett", der u. a. die auflagenstärkste Tageszeitung „US Today" herausbringt.

The Journal News kannte die Bedenken zur Privatsphäre im Hinblick auf die Veröffentlichung. In einem fünfseitigen Bericht der Lokalzeitung kommt ein Staatsbediensteter, Paul Piperato, zu Wort: „Unter den Genannten sind Richter, Polizisten im Ruhestand und FBI Agenten. Wenn man der Öffentlichkeit verrät, wo sie wohnen, bringt man sie in Gefahr." Dafür, dass die Zeitung dieses Risiko bewusst in Kauf nahm, wurde sie harsch kritisiert. In hunderten Kommentaren wurde moniert, dass kaum journalistische Arbeit, sondern einfach eine Anfrage bei der Behörde und „Copy-and-Paste" hinter Artikel und Grafik stecke. Ein Online-Kommentar: „Warum sollte ich wissen wollen, wo die Leute wohnen, die legal Waffen besitzen?" „Was mich interessieren würde, wäre eine Karte, die die illegalen Schusswaffen zeigt", kommentierte eine Wendy Mierbeth, deren Eltern ebenfalls auf der Karte auftauchen, allerdings, wie sie verwundert bemerkt, mit nur einer Waffe. Die Zeitung berief sich bei ihrer Behördenanfrage auf den seit 1966 geltenden „Freedom of Information Act". Keine Angaben waren zumeist darüber zu entlocken, wie viele Schusswaffen und welche Kaliber gemeldet sind. Die Ämter reagierten sehr unterschiedlich auf die Presseanfrage der Zeitung, die sich bereits 2006 mit einer ähnlichen Aktion den Zorn der Waffen-FreundInnen zugezogen hatte. Im Bezirk Putnam etwa erhielt die Lokalzeitung nur die Auskunft, es gebe etwa 11.000 Waffenscheine. Wer diese halte, könne man nicht sagen; das sei zu zeitaufwendig.

Auch die Datensätze aus Rockland und Westchester sind unterschiedlich aussagekräftig. Während sich unter den 16.998 Waffenschein-Inhabenden Rocklands auch Tote und längst Weitergezogene befanden, handelte es sich bei den 16.616 WaffenbesitzerInnen Westchesters um Menschen, die in den vergangenen fünf Jahren ihre Lizenz erneuert oder für einen Waffenkauf gebraucht haben. Ein Großteil der veröffentlichten Personen sind Hobby-Schützen und Jäger. Etwa ein Sechstel, also rund 2.300 Personen, braucht die Waffe aus beruflichen Gründen. Tom King, Präsident der die Waffenlobby vertretenden New York Rifle & Pistol Association (NRA), kritisierte: „Sie geben Kriminellen eine Einkaufsliste an die Hand." Wo es keine Waffen(scheine) gebe, lasse sich gefahrlos einbrechen. In Reaktion auf die Aktion wurden Namen und Adressen der Zeitungsredakteure im Internet veröffentlicht. Auch viele WaffenskeptikerInnen äußerten ihre Probleme damit, Menschen ohne ihr Einverständnis im Internet zu outen. Andere meinten, für Eltern sei es wichtig zu wissen, in welchem Haushalt es Waffen gebe; so könnten sie entscheiden, ob sie ihren Kindern erlauben, dorthin eine Einladung zum Geburtstag oder zum Spielen anzunehmen.

The Journal News verteidigte die Aktion. Die Chefin der Journal News Media Group, Janet Hasson, erklärte, dass es die Zeitung für ihre Aufgabe halte, öffentlich zugängliche Informationen zu publizieren, auch, wenn man sich damit unpopulär mache. Al Tompkins von der Journalistenschule The Poynter Institute in Florida bezeichnete dagegen das Vorgehen als „ungerechtfertigt". Man gebe die Waffenbesitzer öffentlichem Spott preis - und missbrauche zudem die generelle Zugänglichkeit staatlicher, nicht vertraulicher Dokumente. Strafbar war das Vorgehen der Lokalzeitung wohl nicht. Zwar gebe es kein Recht auf die nun veröffentlichten Informationen. Eine Regelung, die die Publikation ausdrücklich verbietet, gebe es jedoch ebenso wenig. Der Bundesstaat New York garantiert per Gesetz, Informationen wie diese innerhalb von zwei Monaten zu erhalten. The Journal News hatte schon nach Tagen erste Ergebnisse. Der Journalist Tompkins verglich das Vorgehen damit, grundlos die Notrufnummer 911 zu wählen oder die Privatadressen von Richtern und Polizisten zu publizieren. Dwight R. Worley, Autor der interaktiven Grafik und des dazugehörigen Artikels, outete sich übrigens in der Veröffentlichung selbst als Waffenbesitzer. In einer Anmerkung der Redaktion über dem Artikel heißt es, er habe eine Smith & Wesson 686.357 Magnum, die seit Februar 2011 in New York City genehmigt sei (Theile, Pistolenfreunde am Internet-Pranger, SZ 28.12.2012, 10; Rüb, Dein Nachbar mit der Waffe, www.faz.net 27.12.2012).

USA

RFID-Schülerortung

Eine texanische High School kontrolliert mit Funkchips, ob ihre SchülerInnen auf dem Schulgelände sind. Eine 15-jährige versuchte erfolglos, sich vor einem Bundesgericht dagegen zur Wehr zu setzen. Die Schülerin aus dem San Antonio North Side School District in Texas und ihre Familie wollten nicht akzeptieren, eine Ausweiskarte mit einem RFID-Chip um den Hals tragen zu müssen. RFID steht für Radio Frequency Identification Device. Mit dem Funkchip kann die John Jay High School über ent-

sprechende Lesegeräte feststellen, ob sich die SchülerInnen bei Unterrichtsbeginn im Schulgebäude aufhalten. Die Klägerin weigerte sich, die Ausweiskarte zu tragen, woraufhin sie suspendiert wurde. Das Gericht hob die Suspendierung zunächst auf, entschied aber abschließend dann doch anders.

Der Grund für den Einsatz der Chips ist finanzieller Natur: Der Schulbezirk bekommt für jede SchülerIn Geld vom Staat – aber nur, wenn die SchülerIn in der Schule ist. Die Anwesenheit wird täglich überprüft. Fehlt einE SchülerIn zu oft, kürzt der Staat die Mittel. Der Schulbezirk argumentierte, er verliere 1,7 Millionen Dollar im Jahr, weil SchülerInnen bei Unterrichtsbeginn zwar schon im Gebäude, nicht aber im Klassenraum seien. Nach anderen Angaben zählt aber schon einE SchülerIn, deren Anwesenheit auf dem Schulgelände per RFID festgestellt wird, als anwesend. Zwei andere Schulbezirke in Houston setzen die Technik seit einigen Jahren ein und berichten von finanziellen Vorteilen in Höhe von mehreren Hunderttausend Dollar.

Auch die John Jay High School überprüft mit dem Ortungschip, wo sich die SchülerInnen tagsüber aufhalten. Ein Bezirkssprecher behauptete, die Software funktioniere nur innerhalb des Schulgebäudes und sei nicht geeignet, SchülerInnen dauerhaft zu verfolgen. Die American Civil Liberties Union (ACLU) ist strikt gegen die Schul-Überwachung: „Wir wollen nicht, dass diese Überwachungsinfrastruktur Eingang in unsere Kultur findet. Wir sollten unseren Kindern nicht beibringen, so eine Technik zu akzeptieren.“ Konservative Politiker halten die Technik für den Ausdruck eines kontrollwütigen Staates. Das Rutherford-Institut, eine Bürgerrechtsorganisation, unterstützt das Mädchen wegen der Verletzung von dessen verfassungsmäßigem Recht auf Privatsphäre.

Das Mädchen und ihre streng christliche Familie argumentierten vor Gericht in erster Linie mit religiösen Überzeugungen, nicht mit dem Überwachungsaspekt. Die Ausweiskarte, die neben dem Chip auch den Namen, ein Foto sowie einen Barcode mit der Sozialversicherungsnummer des jeweiligen Schülers enthält, sei ein „Teufelszeichen“. Es erinnere sie an die Offenbarung des Johannes, in der es heißt: „Und es macht, dass die Kleinen und die Großen, die Reichen und die Armen, die Freien und die Knechte – allesamt sich ein Malzeichen geben an ihre rechte Hand oder an ihre Stirn, dass niemand kaufen oder verkaufen kann, er habe denn das Malzeichen, nämlich den Namen des Tiers oder die Zahl seines Namens. Hier ist Weisheit! Wer Verstand hat, der überlege die Zahl des Tiers; denn es ist eines Menschen Zahl, und seine Zahl ist 666.“

Das Mädchen hatte die Ausweiskarte früher bereits getragen, als diese noch keinen Chip enthielt. Das Angebot der Schule, einfach den RFID-Chip in ihrer Karte zu entfernen, lehnt die Familie trotzdem als unzureichend ab. Die Nutzung der Karte sei als stillschweigende Unterstützung des RFID-Programms zu betrachten. Die Familie forderte die Schule auf, das RFID-Programm komplett zu stoppen. Der Richter am zuständigen Bundesgericht hielt das Angebot des Schulbezirks aber für angemessen; die religiösen Bedenken würden damit ausgeräumt. Die Betroffene will mit Unterstützung des Rutherford-Instituts in Berufung gehen (Beuth, Wie sich eine Schülerin gegen Überwachung wehren wollte, www.zeit.de 09.01.2013).

USA

Automatisierter Echtzeit-Wahrheitscheck

Die US-Zeitung „Washington Post“ hat Ende Januar 2013 den Prototyp einer Software vorgestellt, die annähernd in Echtzeit als Lügendetektor für die politische Debatte funktionieren soll. Das Programm „Truth Teller“ kann automatisch Transkripte von Politikerreden oder Talkshow-Diskussionen erstellen, deren sachlichen Gehalt ein Algorithmus mit Datenbanken und Archiven abgleicht. Über einer Äußerung leuchten dann entweder die Wörter „wahr“ oder „falsch“ auf. Unter truthteller.washingtonpost.com kann man sich erste Eindrücke verschaffen, die allerdings zunächst nur auf einige ausgewählte Beispiele aus der aktuellen amerikanischen Debatte um eine Steuerreform beschränkt sind.

Die Zeitung hat den Wahrheitscheck mit Hilfe von Geldern der Knight Foundation, einer Stiftung, deren Aufgabe die Förderung von Qualitätsjournalismus ist, entwickelt. Es sei das erklärte Ziel, den Truth Teller schließlich als App für das Smartphone anzubieten, so dass in Zukunft einmal die Zuhörer von Politikerreden vielleicht noch während einer laufenden Wahlkampfveranstaltung erkennen können, ob der Inhalt der Rede zutrifft oder nicht.

Noch patzt der Prototyp, der in nur drei Monaten entwickelt wurde, ein wenig bei der Wahrheitsfindung. Wenn etwa der demokratische Kongressabgeordnete Gerald Connolly Präsident Obama in einer Rede dafür preist, dass er die Steuern für 95% der Amerikaner gesenkt habe, dann bewertet der Truth Teller diese Aussage als falsch. Die hierzu angegebene Quelle, der von Menschenhand vollzogene Faktencheck der Seite Politifact.com, kommt aber zum Schluss, sie sei zumindest „halb-wahr“. Für Nuancen aus der Welt des Nicht-Binären scheint der Wahrheitsfinder bislang nicht gemacht.

Schon bewiesen hat der Truth Teller allerdings den rasanten Aufstieg des Faktencheckers zur letzten Instanz der öffentlichen Debatte. Längst sind in den Medien Schiedsrichter allgegenwärtig, die vermeintlich streng nach Tatsachenlage den Daumen über Politikeräußerungen heben oder senken. So datenbasiert und postideologisch, wie sich die Netzöffentlichkeit gerne sieht. Dem gegenüber steht eine politische Klasse, deren Mitglieder vor allem auf Seiten der Republikaner längst nicht mehr „in einer evidenzbasierten Welt leben wollen“, wie es die scheidende Außenministerin Hillary Clinton so schön formulierte (Hofmann, Echtzeit-Wahrheitscheck für die politische Debatte, www.sueddeutsche.de 04.02.2013).

USA

10 Jahre Haft für Hackerazzi

Ab Herbst 2010 tauchten im Internet Dutzende intime Fotos, Drehbücher und private Gespräche von Hollywoodstars im Internet auf. Die Schauspielerin

Mila Kunis war nackt in der Wanne badend zu sehen. Deren Kollegin Scarlett Johansson räkelte sich unbekleidet auf einem Bett. Als Talkgast bei David Lettermann erklärte Johansson kurz später im Fernsehen, wie schockiert sie war, als sie die Bilder entdeckte, die eigentlich nur für die Augen ihres damaligen Ehemanns Ryan Reynolds bestimmt gewesen seien. Jemand müsse ihren Yahoo-Mail-Account geknackt und die Fotos gestohlen haben. Johansson hatte die Bilder selbst zu Hause vor einem Spiegel mit einer Handykamera aufgenommen.

Nach 11 Monaten Ermittlungen der „Operation Hackerazzi" des Federal Bureau of Investigation (FBI) wurde der 35-jähriger Arbeitslose Christopher Chaney überführt und im Dezember 2012 in Los Angeles zu zehn Jahren Haft verurteilt, unter anderem wegen der Verletzung von Persönlichkeitsrechten und dem illegalen Abhören und Beschädigen von Computern. Außerdem muss er 76.000 Dollar Strafe zahlen. Chaney hatte gestanden, mehr als 50 Opfer, darunter Johansson, Kunis und Christina Aguilera, von November 2010 bis Oktober 2011 ausspioniert zu haben und intime Fotos und private Gespräche an andere Hacker sowie Klatschportale weitergegeben zu haben. Richter S. James Otero begründete das Urteil damit, der Angeklagte habe seinen Opfern mit dem Eindringen in deren Privatsphäre eine „unglaubliche Missachtung" entgegengebracht. Er hatte Zugang zu sämtlichen E-Mails seiner Opfer sowie zu deren „persönlichsten Informationen". Staatsanwalt Andre Birotte jr. sieht den Fall als eine Mahnung an alle Internetnutzenden, ihre Identität und persönlichen Informationen im Netz zu schützen.

Um an die Daten zu kommen, hatte Chaney laut FBI keine ausgefeilten oder gar komplizierten Hackertechniken nutzen müssen. Die öffentlich zugänglichen Informationen genügten für seine Angriffe. Chaney rief einfach die Webseiten von gängigen E-Mail-Providern auf und probierte aus. Recht schnell passten zu den vermuteten E-Mail-Adressen der Prominenten geratene Passwörter. Manchmal waren es Filmtitel oder Geburtsdaten, ein anderes mal der Namen des Freundes oder der des Hundes. Hatte er sich Zugang auf einen E-Mail-Account verschafft, kopierte er die Adressbücher der Opfer und änderte die Einstellungen so, dass sämtliche eingehenden Nachrichten an eine E-Mail-Adresse umgeleitet wurden, auf die er zugreifen konnte. Für die Weitergabe der Fotos, Nachrichten und Drehbücher hatte Chaney kein Geld verlangt. Er hat auch nie den Versuch unternommen, seine Opfer mit dem intimen Material zu erpressen. Der Fall löste in den USA eine Debatte aus, ob es im Zeitalter von Facebook und Twitter wirklich nötig ist, jede noch so nichtige Lebensregung über soziale Netzwerke zu verbreiten, was Reize setze, von denen offenbar Chaney profitierte. Scarlett Johansson nimmt ihre Nacktfotos im Internet mittlerweile mit Humor. Nach Festnahme des Täters erklärte sie, dieser habe ihre Schokoladenseiten erwischt (Hauck, Privatsache, SZ 19.12.2012, 9).

USA

Kalifornisches Gericht stoppt Internet-Offenlegungspflicht von Sexualstraftätern

Ein Bundesgericht in San Francisco hat dem US-Bundesstaat Kalifornien am 11.01.2013 untersagt, eine neue Vorschrift umzusetzen, wonach Sexualstraftäter all ihre Internet-Identitäten der Polizei mitteilen sollen. Die Regelung ist Teil eines Gesetzespakets zur Bekämpfung von Menschenhandel und Zwangsprostitution, über das die BürgerInnen Kaliforniens bei der Wahl im November 2012 abgestimmt hatten. Der „Proposition 35" zufolge sollen Menschenhändler oder Zuhälter als Sexualstraftäter registriert werden und ihre Nutzerdaten von Online-Diensten den Behörden mitteilen. Diese Offenlegungspflicht ist auch für alle anderen Sexualstraftaten vorgesehen.

Richter Thelton Henderson sah in der Regelung eine Einschränkung des Rechts auf freie Meinungsäußerung der Betroffenen, die sich im Netz auch anonym zu verschiedensten Themen äußern können müssten. Für die öffentliche Sicherheit ergäbe sich durch diese Regelung nur ein geringer Nutzen. Das Gesetz würde die zuständigen Polizisten nicht davon abhalten, die so erlangten Informationen öffentlich zu machen. Der Beschluss richtet sich nur gegen die Herausgabepflicht der Zugangsdaten; die anderen Regelungen des Gesetzes bleiben anwendbar. Gegen die Entscheidung kann Berufung eingelegt werden.

Der Gesetzesinitiative hatten Anfang November 2012 81% der WählerInnen in einer Abstimmung parallel zur Wahl des kalifornischen Parlaments sowie des US-Präsidenten zugestimmt. Auf die Klage zweier Sexualstraftäter und einer Bürgerrechtsgruppe hin hatte Richter Henderson die Offenlegungspflicht bereits am 07.11.2012 vorübergehend ausgesetzt. In Kalifornien hätten ansonsten rund 73.000 Personen der Polizei ihre Internetadressen, ihre Benutzernamen im Netz und ihren Internet-Provider mitteilen müssen. Die Unterstützenden des Gesetzespakets zeigten sich enttäuscht. Die Anwältin der Kläger meinte, es sei ein wichtiges Ziel, Zwangsprostitution zu stoppen; eine Einschränkung der Redefreiheit im Netz sei aber nicht der richtige Weg. Der Umgang mit diesem Thema wird in den USA häufig diskutiert. Verurteilte Sexualstraftäter müssen in Lousiana seit August 2012 in sozialen Netzwerken ihre Verbrechen offenbaren (Kalifornisches Bundesgericht stoppt Internetregeln für Sexualstraftäter, www.heise.de 14.01.2013).

USA

Instagram ändert AGB zulasten der Nutzenden

Das US-Facebook-Tochterunternehmen, der Online-Fotodienst Instagram wollte sich ab dem Januar 2013 weitgehende Rechte zur Verwendung von Nutzerdaten und ihren Fotos für Werbezwecke einräumen. Nach heftiger öffentlicher Kritik teilte Firmenmitbegründer Kevin Systrom am 20.12.2012 mit, dass hierauf verzichtet werde. Im Firmenblog entschuldigt sich Systrom dafür, die Absichten von Instagram nicht klar genug kommuniziert zu haben. Die Rückmeldungen der Nutzenden hätten ihn dazu bewo-

gen, die geplanten Neuformulierungen über die Verwendung von Nutzerdaten zu Werbezwecken zu streichen und bei der bisherigen Version vorerst zu bleiben.

Bislang heißt es in den Nutzungsbedingungen von Instagram zum Thema Werbung: „Sie sind damit einverstanden, dass Instagram Werbung in seinen Diensten oder in Verbindung mit Ihren Inhalten platziert.“ Schon jetzt erlaubt sich Instagram also, Werbung im Umfeld der Nutzerinhalte einzublenden. An dieser Formulierung hatten sich die NutzerInnen bislang nicht gestört. In den neuen AGB sollte es dann heißen: „Sie sind damit einverstanden, dass ein Unternehmen oder eine Einrichtung uns bezahlt, damit wir Ihren Benutzernamen, Ihre Fotos inklusive deren Metadaten und/oder Ihrer Aktionen bei Instagram in Verbindung mit bezahltem oder gesponsertem Inhalt anzeigen, ohne jede Bezahlung für Sie.“ Das klingt nach einer Übernahme des Prinzips der „gesponserten Meldungen“ auf Facebook: Wer auf einer teilnehmenden Firmenseite auf „Gefällt mir“ klickt, generiert damit - möglicherweise ohne es zu merken - eine Facebook-Anzeige für seine Freunde, die seinen Namen und sein Foto im Zusammenhang mit der Firma zeigt. Die Formulierung von Instagram wurde von vielen als Freifahrtschein für das Unternehmen interpretiert, die von Nutzern hochgeladenen Fotos ungefragt und ohne Bezahlung an Dritte zu verkaufen.

Um klarzumachen, dass dies ausgeschlossen ist, soll nun weiterhin die alte Version dieses Abschnitts gelten, jedenfalls so lange, bis Instagram sich genau überlegt hat, wie Werbung auf der Foto-Plattform funktionieren soll. Dann werde man erneut auf die Nutzer zugehen und es ihnen erklären, schrieb Systrom. Nicht explizit teilte er mit, dass nicht alle neuen Formulierungen rückgängig gemacht wurden. So steht in den seit dem 19.01.2013 geltenden Regeln weiterhin, dass Werbung innerhalb des Dienstes nicht immer als solche kenntlich gemacht wird. Ebenfalls erhalten bleibt der neue Punkt 3 der Basic Terms: Instagram-Nutzende müssen sicherstellen, dass alle persönlichen Angaben, die sie bei der Registrierung oder später machen, „wahr, akkurat, korrekt und vollständig“ sind. Das klingt nach der viel kritisierten Klarnamen-Politik von Facebook, auch wenn die Verwendung eines Pseudonyms weiterhin möglich ist. Zumindest will die Facebook-Tochter aber bei der Anmeldung „echte“ Daten haben, damit das Instagram-Konto leichter mit dem Facebook-Profil verknüpft werden kann.

Auch an den Plänen, Anmeldedaten, Daten aus Cookies, Log-Files sowie Metadaten aus hochgeladenen Fotos mit Facebook zu teilen, ändert sich nichts. Andernfalls hätte Facebook wenig vom Kauf der Plattform gehabt. Facebook hatte im April 2012 für Instagram fast eine Millarde Dollar bezahlt. Instagram mit seinen ca. 100 Millionen Nutzenden selbst macht keine Gewinne, von denen Facebook profitieren würde, doch kann Facebook die Instagram-Nutzerdaten mit seinen eigenen Beständen verknüpfen, um noch mehr personalisierte Werbung innerhalb seiner Angebote zu verteilen.

Gegen die neuen Nutzungs- und Datenschutzbestimmungen von Instagram wurde in den USA am 23.12.2012 eine Sammelklage bei einem Bundesgericht in San Francisco eingereicht, wie die kalifornische Anwaltskanzlei Finkelstein und Krinsk mitteilte: „Instagram nimmt seinen Nutzern ihre Rechte, während es sich selbst von jeder Verantwortung abschirmt.“ In der Klageschrift heißt es, Instagram habe seine Pläne nicht vollständig zurückgenommen, sondern die Regeln nur zu PR-Zwecken umformuliert. Außerdem solle sichergestellt werden, dass Instagram-Nutzer, die sich von dem Onlinedienst abwendeten, weiterhin alle Rechte über ihre dort veröffentlichten Bilder behielten. Die Anwaltskanzlei betonte, dass sich Zehntausende Instagram-Nutzende im Bundesstaat Kalifornien der Sammelklage anschließen könnten. Der Instagram-Mutterkonzern Facebook sagte dazu, die Klage sei „wertlos“. „Wir werden sie energisch bekämpfen“ (Beuth, Instagram bleibt bei seinen alten AGB - aber nur teilweise, www.zeit.de 21.12.2012; Nutzer in Kalifornien verklagen Instagram, www.zeit.de 25.12.2012; Koch, Verwackelt, SZ 27.12.2012, 22).

USA

200 Mio. Dollar für Kartenbetrüger

Die US-Polizei hat einen extremen Fall von Kreditkartenbetrug aufgedeckt. 13 Verdächtige sollen sich nach Mitteilung des US-Justizministeriums vom 05.02.2013 mit ausgeklügelten Methoden mindestens 200 Millionen Dollar (147 Millionen Euro) ergaunert haben. Sie hätten Tausende falsche Identitäten erfunden und damit rund 25.000 Kreditkartenkonten eröffnet. Mit einem Geflecht aus Scheinfirmen, Bankkonten in aller Welt und KomplizInnen in mittelständischen Geschäften hätten sie über Jahre immense Schulden aufgebaut - ohne die Absicht, sie jemals zurückzuzahlen. Mit dem Geld hätten sich die Verdächtigen Luxusautos, teure Kleidung und Unterhaltungselektronik gekauft. Zudem legten sie das Geld in Gold an und verschoben es ins Ausland. Die Staatsanwaltschaft spricht von einem „extravaganten Lebensstil“. Bei einem Verdächtigen seien 70.000 Dollar im Ofen gefunden worden. Viele der TäterInnen seien in den vergangenen fünf Jahren keiner geregelten Arbeit nachgegangen. Die Ermittlungen der Polizei hätten bis zu den Verhaftungen am Tag der Bekanntgabe eineinhalb Jahre gedauert. Insgesamt gebe es 18 Angeklagte (Kreditkartenbetrüger erbeuten 200 Millionen Dollar, www.stern.de 06.02.2013).

Großbritannien/Australien

Nach unsensiblem „Scherzanruf“ Selbstmord

Am 06.12.2012 wurde Kate, Herzogin von Cambridge und Ehefrau vom in der britischen Thronfolge stehenden William aus dem King Edward VII. Hospital entlassen. Vorausgegangen war eine gnadenlose Boulevard-Berichterstattung über deren Schwangerschaftsübelkeit. Ein Tag darauf war die indische Krankenschwester Jacintha S. tot, was einen neuen Medienhype auslöste. Zwei beim australischen Radiosender „2DayFM“ tätige ModeratorInnen hatten zwei Tage zu-

vor bei dem Krankenhaus angerufen und sich am Telefon mit verstellten Stimmen als Queen Elizabeth II. und Prinz Charles ausgegeben und sich nach dem Gesundheitszustand von Kate erkundigt. Jacintha S. hatte den Anruf entgegengenommen und ihn an die diensthabende Schwester durchgestellt, der die beiden Anrufenden dann vertrauliche Details entlockten. Das aufgezeichnete Telefonat wurde vom Sender immer wieder gesendet, über den Tod der Krankenschwester hinaus. In den Tagen danach beschrieben KollegInnen von Jacintha S. diese als „einsam und verwirrt“. Jacintha S., die einen Scherzanruf im Krankenhaus mit der schwangeren Kate weitergeleitet hatte, hat sich, so der Untersuchungsbericht der Londoner Polizei vom 13.12.2012, erhängt.

Die Frau habe zudem Verletzungen an den Handgelenken gehabt.

Lord Glenarthur, Chef des Krankenhauses, wandte sich in scharfer Form an die Betreiber von 2DayFM Southern Cross Austereo: Die unmittelbaren Folgen des „vorsätzlichen und törichten Vorgehens“ der beiden Moderatoren sei die „Demütigung zweier engagierter und fürsorglicher Krankenschwestern“ gewesen. „Die längerfristigen Konsequenzen seien unaussprechlich tragisch“. Es sei „absolut abstoßend“, dass das Management des Senders die Ausstrahlung des Gesprächs durchgewinkt habe. Der angerichtete Schaden könne „nicht mehr ungeschehen gemacht werden“. 2DayFM zeigte sich reumütig, sprach von einer „Tragödie“ und nahm die verantwortlichen Moderatoren vorerst vom Sender. Rhys Hollera, Vorstand von Southern Cross Austereo, meinte, die beiden seien „am Boden zerstört“. Dem australischen Radiosender drohen Konsequenzen aus dem Anruf. Die australische Medienaufsicht leitete am 13.12. eine formelle Untersuchung ein, ob 2DayFM mit dem Anruf die Richtlinien für Privatsender verletzt habe.

Phil Mercer, Australien-Korrespondent der BBC, beschreibt die Gepflogenheiten bei australischen Sendern als „haarsträubend“; der Umgangston sei bisweilen „extrem anzüglich“. Dies sei Folge des „harten Kampfes um Anzeigenkunden“. Nicht erklärt wurde, weshalb die beiden Krankenschwestern vor der Ausstrahlung des Telefonats nicht benachrichtigt wurden, so wie dies das australische Gesetz verlangt hätte. Die Facebook-Seite von 2DayFM wurde am Tag nach dem Tod von Jacintha S. mit Schmähnachrichten bombardiert. Die australische Presse äußerte dagegen eine Art Verständnis für den „Scherz“. So glaubte der Leitartikler von Rupert Murdochs „Sunday Telegraph“ nicht, dass die Moderatoren „irgendjemanden verletzen wollten“. Unter der Überschrift „Trauern, nicht beschuldigen“ schrieb er: „Telefonstreiche sind einer der ältesten Radiotricks. Bisweilen lustig, bisweilen peinlich, haben sie in der Regel nichts weiter als die sinnlose Demütigung eines unglücklichen Opfers zur Folge“ (Menden, Gnadenlos, SZ 20.12.2012, 10; Autopsie-Bericht: Kates Krankenschwester erhängte sich, http://www.augsburger-allgemeine.de 13.12.2012).

Russland

Geld abheben mit Fingerabdruck

Die russische Bank Leto führt als erste im Land im Jahr 2013 das Geldabheben mit dem Fingerabdruck zur individuellen Identifizierung ein. Nach Eingabe der persönlichen Geheimnummer wird das Geld ausgegeben. Eine Bankkarte ist nicht nötig. Die Bank ist eine vor kurzem gegründete Tochter der Großbank VTB, die sich vor allem um Mikrokredite kümmern möchte (Russland-heute 05.12.2012, 3).

Neuseeland

Von Europäischer Union als „sicherer Datenhafen“ anerkannt

Die Kommission der Europäischen Union (EU) bescheinigte Neuseeland am 19.12.2012 offiziell, dass dort europäische personenbezogene Daten angemessen geschützt werden. Dies erleichtert die grenzüberschreitende Übermittlung von personenbezogenen Daten und damit auch den Handel. Davon könnten, so die Kommission, Anbieter sozialer Netzwerke oder von Cloud-Computing-Diensten profitieren, da sie nun Rechtssicherheit haben, dass europäische Datenschutzvorgaben eingehalten werden. Die EU-Datenschutzrichtlinie von 1995 sieht vor, dass personenbezogene Daten in Drittstaaten nur bei Vorliegen eines angemessenen Schutzes transferiert werden dürfen. Rechtliche Standards, die von unabhängiger Seite zu überwachen sind, müssen garantieren, dass die europäischen Bestimmungen beachtet werden. Wenn die EU-Kommission dies bescheinigt, sind keine zusätzlichen Sicherheitsvorkehrungen mehr nötig, wenn persönliche Informationen übertragen werden.

Vergleichbare Bescheinigungen hat die Kommission zuvor Andorra, Argentinien, Australien, den Färöer-Inseln, Guernsey, Israel, der Isle of Man, Jersey, Kanada, der Schweiz und Uruguay ausgestellt. Justizkommissarin Viviane Reding erklärte, die EU arbeite derzeit an einer umfassenden Datenschutzreform, müsse aber parallel dazu dafür sorgen, dass die Daten von EU-BürgerInnen auch bei Übertragungen in Drittländer sicher seien. Der Beschluss stelle daher einen weiteren Schritt dar, um hohe Schutzbestimmungen „auf globaler Ebene“ zu verankern. Das Testat für Neuseeland unterscheidet sich von dem umstrittenen Safe-Harbor-Abkommen mit den USA. Danach können sich Konzerne wie Google oder Facebook unter Einschaltung eines Dienstleisters einen angemessenen Datenschutz zertifizieren lassen. Europäische DatenschützerInnen sehen das Safe-Harbor-Abkommen als „eine Art Freibrief für die Amerikaner“ an und halten es für wenig aussagekräftig (Krempl, EU erkennt Neuseeland als „sicheren Datenhafen“ an, www.heise.de 19.12.2012).

China

Hack gegen „New York Times“ wegen Berichterstattung

Die „New York Times“ wurde von Hackern aus China ausspioniert. Anlass waren möglicherweise Berichte der Zeitung, die Pekings Machtwechsel 2012 empfindlich störten. Darin hatte die New York Times die Vermögensverhältnisse einiger Topkader offengelegt. Der

Shanghaier Times-Bürochef David Barboza hatte über den immensen Reichtum der Familie des seinerzeitigen Noch-Premier Wen Jiabao berichtet – die Nr. 2 im Staat. Am spektakulärsten war wohl der Bericht über die Verwandten Wen Jiabaos und über die Vermögen der Familie von Xi Jinping, damals noch Vizepräsident, heute Parteichef und damit die Nr. 1 in China. Es ist wohl kein Zufall, dass chinesische Hacker Rechner der New York Times infiltriert haben und zuvor auch die Rechner von Bloomberg-Mitarbeitern; der Dienst hatte ebenfalls berichtet. Die Times veröffentlichte einen recht offenen Bericht über die Rechner-Attacken gegen sich in den vergangenen Monaten. Kaum standen die Times-Berichte online, wurden sie von der chinesischen Zensur gekappt. Dennoch verbreiteten sich die Informationen über Chinas Dienst Weibo weiter. Dass diese Hacks politisch motiviert waren, zeigt die Tatsache, dass laut Times nur nach Informationen im Zusammenhang mit dem Wen-Bericht gesucht wurde, Nutzerdaten seien nicht abgezogen worden. Begonnen habe der Rechnerangriff laut New York Times bereits Mitte September 2012, also rund sechs Wochen vor der Veröffentlichung des Artikels. Auftragshacker hätten zu diesem Zeitpunkt Schadsoftware auf den Computern von mehreren Redakteuren platziert und diese ausspioniert.

Wie sie das genau geschafft hatten, ist noch nicht bekannt. Wahrscheinlich hätten sie die Spear-Phishing-Methode angewandt: Einzelne Redakteure hatten offenbar E-Mails bekommen, die sehr genau auf ihre Interessen zugeschnitten waren. In den Anhängen dieser E-Mails war die Schadsoftware versteckt. Über sie wurde wiederum Spähsoftware nachgeladen, die von Screenshots bis zu Tastatureingaben so ziemlich alles aufnehmen und zum Server der Angreifer schicken kann. Mithilfe der Spähsoftware richteten sich die Angreifer mehrere Hintertüren zu den Computern der Redakteure ein. Die abgefangenen Passwörter und andere Hinweise reichten aus, um sich zwei Wochen lang im Netzwerk der Zeitung umzusehen. Dabei entdeckten die Angreifer den sogenannten Domain Controller, also den zentralen Rechner, über den sich alle Mitarbeitenden eines Firmennetzes anmelden. Der Domain Controller enthält die Benutzernamen und die zugehörigen Passwörter, Letztere in Form eines Hash-Werts. Über Massenabfragen könne solche Hashs wieder entschlüsselt werden, sodass die Passwörter im Klartext vorlagen. Um diese Angriffe zu verschleiern, nutzten die Hacker kompromittierte Server mehrerer US-Universitäten. Dieses Vorgehen kennen Sicherheitsspezialisten schon von früheren Hacks, die sie einer chinesischen Gruppe mit Verbindungen zum Militär zuschreiben.

Auf diesem Wege bekamen die Angreifer Zugang zu 53 Computern von Times-Angestellten. Für die Rechner des Bürochefs in Shanghai und den des Südostasien-Bürochefs schrieben sie spezielle Spionagesoftware, um den E-Mail-Verkehr der beiden mitlesen zu können. So wollten die Angreifer offenbar herausfinden, wer die Quellen für den Wen-Bericht waren. Insgesamt wurden 45 solcher Programme auf den Computern der Times gefunden, die hauseigene Antivirussoftware der Firma Symantec hatte davon nur eines entdeckt. Die Zeitung bekam von dem Angriff deshalb zunächst nichts mit. Erst, als sie von chinesischen Regierungsbeamten erfuhr, dass ihre Recherche zu den Reichtümern der Familie von Wen „Konsequenzen haben“ würde, reagierte sie: Am Tag vor der Veröffentlichung des Artikels bat die Times ihren Provider AT&T, nach ungewöhnlichen Aktivitäten im Netzwerk der Zeitung zu suchen.

Am Tag der Veröffentlichung meldete AT&T bestimmte Aktivitäten, wie sie bereits von anderen Angriffen bekannt waren, die wahrscheinlich vom chinesischen Militär verübt wurden. Die Times und AT&T versuchten dann, die Eindringlinge wieder aus ihrem Netzwerk zu bekommen, ohne dabei aber das Ausmaß des Angriffs zu erkennen. Als knapp zwei Wochen später klar war, dass die Angreifer weiterhin im System waren, beauftragte das Medienhaus die Firma Mandiant mit der Abwehr. Die halfen dabei, die Machart der Attacke zu verstehen und das Netzwerk gegen weitere derartige Angriffe abzusichern. Drei Monate lang beobachtete die Zeitung die Schnüffelaktion, bevor sie an die Öffentlichkeit ging. Gänzlich sicher kann ein System nicht sein, so lange die Benutzenden verseuchte E-Mails öffnen.

Ein Grund für die Attacken dürfte im Zeitpunkt der Veröffentlichungen liegen. 2012 wechselte die Parteielite ihre Führung aus. Es war die Zeit, als in der Nomenklatura ein unübersehbarer Machtkampf herrschte. Beide Politiker, Wen Jiabao und Xi Jinping, über deren Familien berichtet wurde, haben den Ruf, integre Menschen zu sein. Wen Jiabao stammt zudem aus einfachen Verhältnissen, er hat in seiner Amtszeit regelmäßig Sozialreformen angemahnt und die Korruptionsbekämpfung hoch auf die Agenda gesetzt, beispielsweise während des Nationalen Volkskongresses 2007. Eine Veröffentlichung über die Anhäufung riesiger Vermögen von Parteifamilien untergräbt solche Ansagen. Zwar hatte Times-Autor David Barboza in seinem Artikel weder Wens Familie, noch ihn selbst irgendwelcher illegaler Aktivitäten bezichtigt. Dennoch hatte Wen Regeln der inneren Parteidisziplin verletzt, wonach er hätte verhindern müssen, dass Verwandte von ihm sich in Geschäftsbereichen engagieren, die seiner Aufsicht unterstehen. Als Premier Chinas dürften das aber praktisch alle Geschäftsfelder sein.

Ein Verstoß gegen die Parteidisziplin wiederum kann in China Karrieren zerstören und im politischen Machtgerangel gegen einen verwendet werden. Der Sturz des prominenten Politbüro-Kandidaten und Populisten Bo Xilai in der Megastadt Chongqing war nur die augenfällige Spitze dieser Auseinandersetzungen. Bo und seine Frau hatten gigantische Vermögen angehäuft, die mit normalen Mitteln aus ihren Posten und Berufen nicht möglich waren (DANA 2/2012, 95). Aus Sicht der Parteiführung gab es also viele Gründe, nach Maulwürfen zu suchen, die Informationen an die freie Presse im Westen weitergeben. Weil in China die soziale Gerechtigkeit mit den kapitalistischen Reformen abgenommen hat und gleichzeitig massive Korruption die Bürger bedrängt, sorgen Veröffentlichungen wie jene der Times in der Pekinger Führung für Nervosität. Chinas Mikroblogs sind heute voll von Berichten über Korruption von meist lokalen Kadern, manche Berichte werden zensiert, andere nicht. Auf die chinesischen Teile der Digitalnetze haben die

Pekinger Behörden Zugriff. Auf die außerhalb des Landes muss im Zweifel auf Hacker zurückgegriffen werden.

Die Regierung in Peking bestreitet, hinter den Angriffen zu stecken, so eine Stellungnahme des Verteidigungsministeriums: „Die chinesischen Gesetze verbieten jegliche Handlung, die die Internetsicherheit beeinträchtigt." Zudem sei es „unprofessionell und haltlos, das chinesische Militär ohne verlässliche Beweise zu beschuldigen, Cyberattacken lanciert zu haben" (Beuth/Richter, Chinas Attacke auf die Ahnungslosen, www.zeit.de 31.01.2013; Giesen, Nacht für Nacht im Tunnel, SZ 01.02.2013, 1, 47).

Technik-Nachrichten

Affektive Informatik im Dienste von Kundenbindung und Sicherheit

Digitale Bild- und Stimmerfassung dient nicht nur dem Erkennen von Personen, sondern auch dem Erkennen bzw. Deuten von deren Emotionen. Die sogenannte affektive Informatik will darüber optimales Einkaufen, höhere Kundenbindung oder mehr Sicherheit erreichen – so das Versprechen von Affectiva, einem amerikanischer Hersteller von Software zur Messung von Emotionen. Mobiltelefone erkennen z. B. anhand unserer Stimme, ob wir müde sind und ein wenig Werbung von Starbucks vielleicht angebracht wäre, Schaufensterpuppen sehen, wie wir auf die neue Modelinie im Schaufenster reagieren. Rosalind Picard, Wissenschaftlerin im Dienste von Affectiva, erläutert: „Das ist keine Zukunftsmusik. Unsere Software kann zum Beispiel mithilfe einer hochauflösenden Kamera Gesichtsausdrücke erkennen und sagen, ob jemand glücklich, aufmerksam, verwirrt oder überrascht ist."

Die dabei genutzte Software wurde von einem Forschungsteam des MIT unter Leitung von Picard entwickelt. Man habe 100.000 Gesichtsausdrücke von Menschen aus verschiedenen Kulturkreisen gesammelt, sodass die Software Affdex durch die Analyse von mehr als zwanzig Gesichtspunkten in der Lage sei, Emotionen zu erkennen. Selbst kulturelle Unterschiede seien kein Problem: „Affdex weiß, dass Japaner in Geschäftsgesprächen dazu neigen, weniger Emotionen zu zeigen als beispielsweise Menschen aus Brasilien." Das Internetunternehmen AOL zeigte sich nach einer Pilotstudie begeistert: Es sei dank affektiver Informatik möglich, eine emotionale Bindung zwischen Internetnutzenden und Marken herzustellen. Auch der Einsatz in Kaufhäusern wird erwogen. Die Software analysiert, wo Produkte oder Reklame platziert werden müssen, damit sie die KundInnen optimal ansprechen. Hierzu werden ProbandInnen mit Sensoren ausgestattet und zum Probeeinkaufen geschickt. Mit Kameras ausgerüstete Schaufensterpuppen spionieren die KundInnen aus und analysieren ihre Gesichtsausdrücke, um herauszufinden, wie sie auf die Waren reagieren.

Einige äußern ethische Bedenken, so z. B. Karsten Weber, Professor für allgemeine Technikwissenschaften an der TU Cottbus: „Wenn wir von unserer rationalen Entscheidung abgebracht werden und hin zu einer emotionalen, womöglich gegen unseren Willen, dann ist das höchst problematisch." Bei Affdex ist man davon überzeugt, dass affektive Informatik zusammen mit einem Körperscanner an Flughäfen die Sicherheit erhöhen kann. Verdächtige Personen könnten schließlich anhand ihres Gesichtsausdruckes enttarnt werden. Der Technikphilosoph Bernhard Irrgang sieht hierin aber nicht nur eine Verletzung von Persönlichkeitsrechten: „Eine Maschine darf keine letzten Entscheidungen treffen." Es sei nicht zu verantworten, wenn ein Mensch aufgrund der falschen Entscheidung einer Maschine bestraft würde.

Picard gesteht ein: „Auch die Programme von Affectiva machen Fehler." Aber: „Am MIT haben wir in einer Studie sogar gezeigt, dass Software besser als Menschen ein lachendes Gesicht von einem frustrierten unterscheiden konnte." Wie hoch genau die Fehlerquote ist, konnte sie aber nicht sagen. Dies sieht Irrgang anders: „Maschinen können nicht emulieren, was wir denken oder was wir fühlen. Sie können immer nur simulieren, was von außen irgendwie schematisierbar ist." Der Psychologieprofessor Arvid Kappas ergänzt: „Wir überschätzen völlig die Bedeutung des Gesichtsausdruckes." Der Ansatz von Systemen wie Affdex sei grundsätzlich falsch. „Ein Lächeln bedeutet nicht automatisch, dass wir glücklich sind" (Paletta, Affektive Informatik will unsere Emotionen deuten, www.zeit.de 14.12.2012).

Technische Rekonstruktion von Stasi-Akten

Seit 2007 arbeitet das Fraunhofer Institut für Produktionsanlagen und Konstruktionstechnik (IPK) an einer Software, die die Unterlagen wiederherstellen soll, die Stasi-Offiziere 1989/90 zerstörten, u. a. 90 Säcke mit zerrissenen und geschredderten Dokumenten der Spionage-Abteilung Hauptverwaltung Aufklärung (HVA). 15.000 Säcke mit zerstörten Stasi-Akten lagern noch in den Magazinen der Stasi-Unterlagen-Behörde. Dort ist man zuversichtlich, 400 Säcke in einem Pilotverfahren 2013 lesbar machen zu können. 2013 soll die groß angelegte Rekonstruktion zerrissener Stasi-Unterlagen per Computer beginnen. Der Bundesbeauftragte für die

Stasi-Unterlagen Roland Jahn meinte: „Wir hoffen, dass die Entwicklung der schwierigen Technik abgeschlossen wird und die Testphase beginnt. Die digital zusammengefügten Dokumente werden die Aufarbeitung voranbringen."

Nach dem Mauerfall hatte die Stasi massenhaft Unterlagen vernichten wollen. Offiziere zerrissen zum Schluss Akten per Hand, weil die Reißwölfe heiß liefen. In Stasi-Befehlen hieß es, dass „belastendes Material zu vernichten und Inoffizielle Mitarbeiter (IM) zu schützen" seien. BürgerrechtlerInnen retteten zahlreiche Dokumente. 15.000 Säcke mit Millionen Schnipseln lagern in Depots. Bislang wurden per Hand anderthalb Millionen Blätter wiederhergestellt. Laut Fraunhofer Institut bräuchten 30 Leute für das manuelle Zusammenfügen aller Schnipsel 600 bis 800 Jahre. Mit speziellen Scannern und der weltweit einzigartigen E-Puzzler-Software sollen künftig per Computer Risskanten, Schrift und Papier zugeordnet und die Fetzen zusammengefügt werden. Mehr als acht Millionen Euro flossen bisher in das Projekt.

Jahn, der früher in der DDR-Opposition aktiv war, erläuterte: „Mit den rekonstruierten Akten kann es einen Schub geben bei der Aufklärung über das Wirken der DDR-Geheimpolizei." Gerade zur Arbeit der Stasi und deren HVA im Westen gebe es große Lücken in den Akten. Vieles sei vernichtet worden. Auch zur Verfolgung von Oppositionellen in der DDR würden neue Erkenntnisse erhofft. Nach den Vorstellungen von Jahn soll die Innovation auch der Öffentlichkeit gezeigt werden. „Dem Fraunhofer-Institut schwebt eine gläserne Rekonstruktion in Haus 18 des früheren Stasi-Ministeriums vor, wenn die Testphase erfolgreich ist." Das riesige Gelände an der Berliner Normannenstraße könne sich so zu einem Campus der Demokratie, zu einem Ort des Lernens am authentischen Ort entwickeln (Brisante Stasi-Akten sollen rekonstruiert werden, www.welt.de 27.12.2012).

Indoor-Navigation wird praxisreif

Google präsentierte ein neues Angebot unter dem Namen „Indoor Maps", mit dem z. B. in Museen oder Einkaufszentren der Weg zum Klo oder zur Kasse angezeigt werden kann. Indoor Maps läuft zunächst nur auf Smartphones mit dem von Google entwickelten Betriebssystem Android. Die Navigationshilfe soll allerdings auch auf andere Smartphones wie z. B. Apples iPhone gebracht werden. Zoomt man an ein Gebäude heran, für das Innenraumkarten verfügbar sind, so blendet die aktuelle Version von Google Maps automatisch eine Übersichtskarte ein. Google setzt dabei auf Partner, die Pläne ihrer Gebäude eigenständig bei Google hochladen können. In Deutschland sind drei Flughäfen – Frankfurt, Köln/Bonn und München – eingebunden. Der Dienst ist zudem für zahlreiche Einkaufszentren verfügbar, für 6 Museen sowie für die Fußballstadien des Hamburger Sportvereins und von Borussia Dortmund.

Angebote gibt es bislang in 10 Staaten. Am ausgefeiltesten ist der Dienst in den USA, wo Google das Angebot 2011 u. a. für Kasinos, Krankenhäuser und Kirchen einführte. Um Orientierungshilfen zu geben, muss eine möglichst genaue Positionsbestimmung der Person, die zu Fuß unterwegs ist, vorgenommen werden Da GPS in geschlossenen Gebäuden nicht zur Verfügung steht, muss Google Funksignale aus der Umgebung auswerten. Über die Stärke und die Richtung des Signals kann die Software auf wenige Meter genau errechnen, wo sich die Person bzw. ihr Gerät befindet. Höhenangaben werden berücksichtigt, so dass sich die Karten automatisch auf das gerade betretene Stockwerk aktualisieren können, sobald in einem mehrstöckigen Gebäude die Etage gewechselt wird.

Das größte technische Problem besteht darin, die Funksignale in den Gebäuden so korrekt wie möglich zu vermessen. Je mehr Leute den Dienst nutzen, umso mehr Nutzenden kann Google über diesen Dienst ortsbasierte Werbung anbieten. Auf dem Display des Smartphones kann z. B. kurz vor Starbucks ein Gutschein für einen Kaffee aufploppen. Wie Google die Positionsdaten der Nutzenden darüber hinausgehend nutzt, ist nicht bekannt.

Ein vergleichbares System haben Ingenieure vom Fraunhofer-Institut für Produktionstechnik und Automatisierung in Stuttgart entwickelt. Dieses Arbeit mit in das Smartphone einzubauenden Sensoren. Sobald das Modul keine GPS-Signale mehr empfängt, messen diese, wohin sich das Gerät bewegt. Gemessen werden die Beschleunigung, die Schrittlänge und die Position des Gerätes zum Erdmagnetfeld. Auch dieses System arbeitet in Kombination mit aus dem Internet herunterzuladenden dreidimensionalen Gebäudeplänen von Messehallen, Flughäfen oder Einkaufszentren (DANA 3/2012, 133; Navi für Innenräume, Der Spiegel 50/2012, 120; Bernau, Google weist den Weg zum Klo, SZ 03.12.2012, 20).

Info für DVD-Mitglieder – Sonderkonditionen Konferenzteilnahmen DuD 2013

Am 17. und 18. Juni findet in Berlin bereits zum 15. Mal die Jahresfachkonferenz DuD statt.
DVD-Mitglieder können zum Sonderpreis von 1195 Euro (statt 1695 EUR) teilnemen, wenn sie sich mit dem Stichwort „DDVD" online anmelden.
Für Personen, die noch nie an der DuD teilgenommen haben, gibt es ein Spezialangebot: sie können bei Angabe des Codes „DVD" für nur 600 Euro (insgesamt für beide Konferenztage) an der Konferenz teilnehmen.

Anmeldung und weitere Informationen:
http://www.computas.de/konferenzen/dud_2013/agenda/agenda.html

Rechtsprechung

BVerfG

Spezielle Rechtsgrundlage für die Dauerobservation von Ex-Gefangenen nötig

Das Bundesverfassungsgericht (BVerfG) entschied mit Beschluss vom 08.11.2012 (Az. 1 BvR 22/12), dass auch in einem verwaltungsgerichtlichen Eilrechtsschutzverfahren hinsichtlich der Rechtmäßigkeit der Dauerobservation eines aus der Sicherungsverwahrung entlassenen 53jährigen Mannes geprüft werden muss, ob sich die Einschätzung von dessen Gefährlichkeit auf hinreichend aktuelle Tatsachengrundlagen stützt. Der Fall wurde deshalb an das Verwaltungsgericht (VG) Freiburg zurückverwiesen. Dass die Verwaltungsgerichte die polizeirechtliche Generalklausel als ausreichende Rechtsgrundlage für die Dauerobservation des Beschwerdeführers angesehen haben, wurde nur noch für eine Übergangszeit akzeptiert. Die Polizei kann auf Grundlage der Generalklausel auf unvorhergesehene Gefahrensituationen auch mit im Grunde genommen näher regelungsbedürftigen Maßnahmen – aber nur vorläufig – reagieren. Auftretende Regelungslücken müssen aber vom Gesetzgeber geschlossen werden.

Die Polizeigesetze der Länder regeln jeweils in einer so genannten Generalklausel (z. B. § 1 i. V. m. § 3 PolG BaWü) die Befugnisse der Polizeibehörden allgemein und in sehr offen formulierter Weise, dass diese zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung diejenigen Maßnahmen treffen, die ihnen nach pflichtgemäßem Ermessen erforderlich erscheinen. Wegen der Unbestimmtheit und Offenheit dürfen auf diese Klausel normalerweise nur Maßnahmen mit geringer Eingriffstiefe gestützt werden. Für besonders schwere Grundrechtseingriffe wie z. B. eine Wohnungsdurchsuchung oder eine Ingewahrsamnahme benötigt die Polizei grundsätzlich spezielle Befugnisnormen, welche die genauen Voraussetzungen und Bedingungen detailliert regeln und damit solche Maßnahmen näher begrenzen (z. B. durch besondere Anforderungen an die Dringlichkeit der Gefahr, an die Art der Gefahr – etwa das Erfordernis einer Leib- oder Lebensgefahr – oder an das Verfahren – etwa das Erfordernis einer vorherigen richterlichen Entscheidung). Das Polizeirecht Baden-Württemberg kennt – ebenso wenig wie die Polizeigesetze der anderen Bundesländer – keine ausdrückliche Rechtsgrundlage für die längerfristige Observation von gefährlichen Personen zum Schutz Dritter.

Das Landgericht S. hatte den Beschwerdeführer im Jahre 1985 wegen zwei Vergewaltigungen zu einer Freiheitsstrafe von fünf Jahren mit anschließender Sicherungsverwahrung verurteilt. Mit Beschluss vom 10.09.2010 erklärte das Oberlandesgericht – im Anschluss an die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte – die Sicherungsverwahrung für erledigt. Mit der Entlassung des Beschwerdeführers aus der Sicherungsverwahrung hat die Polizeidirektion Freiburg die längerfristige Observation des Beschwerdeführers zunächst für die Dauer von vier Wochen angeordnet und diese Anordnung seither regelmäßig, insgesamt über mehr als zwei Jahre, verlängert.

Dabei parkte ein Polizeifahrzeug mit drei Polizeibeamten ständig im Hof vor dem Hinterhaus, in dem der Beschwerdeführer ein Zimmer bewohnte. Zwei weitere Beamte hielten sich in der Küche der Unterkunft auf, wenn sich der Beschwerdeführer in seinem Zimmer befand. Eine direkte Beobachtung des Beschwerdeführers in seinem eigentlichen Wohnraum fand nicht statt. Außerhalb seiner Wohnung begleiteten Polizisten den Beschwerdeführer ständig. Bei Gesprächen mit Ärzten, Rechtsanwälten und Bediensteten von Behörden waren die Beamten angewiesen, Abstand zu halten. Nahm der Beschwerdeführer ansonsten Kontakt zu Frauen auf, wiesen die Polizisten sie mit einer so genannten Gefährdetenansprache auf den Grund der Observation hin.

Das VG Freiburg lehnte mit Beschluss vom 16.08.2011 einen Antrag auf einstweilige Anordnung gegen die Observation ab. Dies wurde vom Verwaltungsgerichtshof Baden-Württemberg mit Beschluss vom 08.11.2011 bestätigt. Das BVerfG gab der Verfassungsbeschwerde gegen diese beiden Beschlüsse statt. Zwar hätten die Verwaltungsgerichte richtig erkannt, dass die dauernde Observation einen schwerwiegenden Grundrechtseingriff darstellt, doch dabei dessen Gewicht nicht ausreichend gewürdigt.

Nicht beanstandet wurde, dass die Verwaltungsgerichte die polizeiliche Generalklausel als noch ausreichende Rechtsgrundlage für die dauerhafte Observation herangezogen haben. Das BVerfG bezweifelte, dass diese undifferenzierte Rechtsgrundlage auf Dauer die Durchführung solcher Observationen trägt. Diese neue Form einer polizeilichen – bisher ungeregelten – Maßnahme bedürfe wegen ihrer weitreichenden Folgen wohl einer ausdrücklichen, detaillierten Ermächtigungsgrundlage. Das BVerfG erhob aber keine durchgreifenden verfassungsrechtlichen Bedenken, dass die Gerichte angesichts des Gewichts der in Frage stehenden Rechtsgüter die vorhandene Grundlage im vorläufigen Rechtsschutzverfahren als noch tragfähig ansahen und die Frage nach der Rechtsgrundlage erst im Hauptsacheverfahren abschließend klären wollten. Die polizeiliche Generalklausel ermögliche es, auf unvorhergesehene Gefahrensituationen auch mit im Grunde genommen näher regelungsbedürftigen Maßnahmen vorläufig zu reagieren, und ermögliche so dem Gesetzgeber, eventuelle Regelungslücken zu schließen. Der müsse dann reagieren oder in Kauf nehmen, dass solche Maßnahmen von den Gerichten auf Dauer als unzulässig angesehen werden.

Das BVerfG hob aber die verwaltungsgerichtlichen Entscheidungen aus einem anderen Grund auf: Die Gerichte hatten ihre Entscheidung maßgeblich auf ein psychiatrisches Gutachten vom 05.03.2010 gestützt, als sich der Beschwerdeführer noch in Sicherungsverwahrung befand. Der Gutachter konnte allenfalls vermuten, wie der Beschwerdeführer sich nach Jahrzehnten der Haft und der Sicherungsverwahrung in Freiheit verhalten würde. Nachdem der Beschwerdeführer aber seit geraumer Zeit unter vollständig veränderten Umständen lebte, durfte eine so weitreichende Entscheidung wie die über die Fortsetzung einer fast durchgehenden polizeilichen Beobachtung nicht auf derart veraltete Vermutungen gestützt werden. (Dauerobservation eines entlassenen Sicherungsverwahrten kann nur vorläufig auf polizeirechtliche Generalklausel gestützt werden, www.bundesverfassungsgericht.de 04.12.2012, www.kostenlose-urteile.de 04.12.2012).

BGH

Ausnahmsweise Verwandten-DNA-Auswertung aus Massengentest

Der 3. Strafsenat des Bundesgerichtshofs (BGH) hat mit Urteil vom 20.12.2012 die Verurteilung eines 16-jährigen Jugendlichen wegen Vergewaltigung zu einer Jugendstrafe von fünf Jahren durch das Landgericht (LG) Osnabrück bestätigt und damit ausnahmsweise die Nutzung der Daten von Verwandten aus einem Massengentest zugelassen (Az. 3 StR 117/12). Das LG Osnabrück war von der Täterschaft des Angeklagten maßgeblich deshalb überzeugt, weil beim Tatopfer, einer 27-jährigen Frau, auf dem T-Shirt Zellmaterial gesichert werden konnte, das mit dem DNA-Identifizierungsmuster des Angeklagten übereinstimmt. Zur Ermittlung des Angeklagten als mutmaßlichem Täter hatten die Ergebnisse einer molekulargenetischen Reihenuntersuchung (§ 81h StPO) geführt, an der ca. 2.400 Männer teilgenommen hatten – unter ihnen der Vater und ein Onkel des Angeklagten. Deren DNA-Identifizierungsmuster stimmten zwar mit dem der Tatspuren nicht vollständig überein, wiesen aber eine so hohe Übereinstimmung auf, dass sie auf eine Verwandtschaft mit dem Täter schließen ließen.

Der Angeklagte hat im Revisionsverfahren insbesondere geltend gemacht, die bei der molekulargenetischen Reihenuntersuchung festgestellten DNA-Identifizierungsmuster hätten nicht auf verwandtschaftliche Ähnlichkeiten abgeglichen und im weiteren Verfahren nicht gegen ihn verwertet werden dürfen. Der BGH stellte fest, dass die bei der Auswertung der Proben festgestellte mögliche verwandtschaftliche Beziehung zwischen dem Vater und dem Onkel des Angeklagten mit dem mutmaßlichen Täter nicht als verdachtsbegründend gegen den Angeklagten hätte verwendet werden dürfen. § 81h Abs. 1 StPO erlaubt den Abgleich von DNA-Identifizierungsmustern nur, soweit dies zur Feststellung erforderlich ist, ob das Spurenmaterial von einem der Teilnehmer der Reihenuntersuchung stammt. Gleichwohl erlaubte das Gericht, dass die Übereinstimmung des DNA-Identifizierungsmusters des Angeklagten mit desjenigen der Tatspur vom Landgericht bei seiner Überzeugungsbildung verwertet werden durfte. Zwar sei dieses Identifizierungsmuster rechtswidrig erlangt worden; denn der ermittlungsrichterliche Beschluss, der die Entnahme von Körperzellen des Angeklagten zur Feststellung dieses Musters anordnete (§ 81a StPO), beruhte auf dem durch die unzulässige Verwendung der Daten aus der DNA-Reihenuntersuchung hergeleiteten Tatverdacht gegen den Angeklagten. Indes führt dies in dem konkret zu entscheidenden Fall bei der gebotenen Gesamtabwägung nicht zu einem Verwertungsverbot. Entscheidend hierfür war der Umstand, dass die Rechtslage zum Umgang mit sog. Beinahe-Treffern bei DNA-Reihenuntersuchungen nach Ansicht des BGH bisher völlig ungeklärt war und das Vorgehen der Ermittlungsbehörden daher noch nicht als willkürliche Missachtung des Gesetzes angesehen werden kann. Der Verfahrensverstoß wiege daher nicht so schwer, dass demgegenüber die Interessen der Allgemeinheit an einer effektiven Strafverfolgung hier zurücktreten müssten.

Die Konsequenz des Urteils ist, dass nach Klärung der Rechtsfrage durch den BGH künftig Proben, die nicht direkt zu einem Treffer führen, für die Strafverfolgung tabu sind. Der BGH-Senatsvorsitzende Jörg Peter Becker erläuterte bei der Urteilsverkündung: „Wir haben hier einen originären Rechtsverstoß.“ Das Verwertungsverbot gelte aber „noch nicht“. Mit dem Verbot für die Zukunft verfolgt der BGH offenbar einen „Disziplinierungsgedanken“. Massengentests sind ohnehin ein aus Datenschutzsicht fragwürdiges Mittel. Oft kommt das Ergebnis nicht über einen Treffer zustande, sondern über das Ausschlussverfahren: Der Kreis der Verdächtigen wird eingegrenzt. Sobald er eng genug ist, dürfen Testverweigerer zur DNA-Abgabe gezwungen werden, wenn weitere Indizien gegen sie sprechen (PM BGH Nr. 216/2012 20.12.2012; Janisch, Die schmale Spur der Gene, SZ 21.12.2012, 6).

BSG

Weitgehende Auskunftsansprüche bestätigt

Gemäß einem Urteil des Bundessozialgerichts (BSG) vom 13.11.2012 müssen Behörden den BürgerInnen umfassend Auskunft geben, welche Daten über sie gespeichert und in welchem Umfang an Dritte weitergegeben wurden (Az. B 1 KR 13/12 R). Der Anspruch umfasst auch die Frage, an wen und mit welchem Medium Daten weitergegeben wurden. Im Streitfall hatte eine schwerkranke Frau aus Rheinland-Pfalz den Verdacht, ihre Krankenkasse AOK habe der Arbeitsagentur und an die Stadt Kaiserslautern ohne ihre Zustimmung Gesundheitsdaten preisgegeben. Ein Rehabilitationsträger habe weit mehr Daten bekommen als nötig. Zudem habe die Krankenkasse ihre Daten offenbar unverschlüsselt per E-Mail verschickt.

Die Frau verlangte von der AOK Rheinland-Pfalz/Saarland Auskunft, wer welche Daten auf welchem Wege bekommen hat. Die AOK lehnte dies unter

Hinweis auf den „unverhältnismäßigen“ Aufwand ab. Das Gericht forderte die Krankenkasse auf, ein Widerspruchsverfahren zuzulassen. Das BSG nahm den Streit zum Anlass, sich umfassend zum datenschutzrechtlichen Auskunftsanspruch zu positionieren. Danach können Behörden in dieser Frage nicht auf einen hohen Verwaltungsaufwand verweisen. Vielmehr müssen sie ihre Dokumentation und ihre Datenverarbeitung so organisieren, dass eine Auskunft mit vertretbarem Aufwand möglich ist. Gegebenenfalls könnten sie den Auskunftsanspruch auch durch Akteneinsicht erfüllen. Die BürgerInnen können auch darüber Auskunft verlangen, an wen und auf welchem Wege Daten weitergegeben wurden.

Umstritten war bislang, ob Behörden auf einen Auskunftsantrag mit einem formellen Verwaltungsakt reagieren müssen. Nach dem Kasseler Urteil ist dies nicht erforderlich, wenn die Auskunft erteilt wird; ein zusätzlicher Bescheid wäre, so das BSG, nur überflüssige Bürokratie. Dagegen muss ein Verwaltungsakt ergehen, wenn der Antrag abgelehnt wird. Dies ermöglicht es den Betroffenen, ein Widerspruchsverfahren einzuleiten und erleichtert gegebenenfalls auch eine Klage vor Gericht. Der Senat hat das Urteil des Landessozialgerichtes (LSG) Rheinland-Pfalz aufgehoben und den Rechtsstreit an das LSG zurückverwiesen, damit die beklagte Krankenkasse im wieder eröffneten Berufungsverfahren das Verfahrenshindernis des Fehlens eines Vorverfahrens beseitigen kann. Richtige Klageart für das Auskunftsbegehren ist die kombinierte Anfechtungs- und Leistungsklage (www.bundessozialgericht.de, 14.11.2013; Gericht stärkt Rechte der Bürger bei Datenweitergabe von Behörden, www.123recht.net).

OLG Hamm

Keine sichere Anonymität für Samenspender

Das Oberlandesgericht (OLG) Hamm hat mit Urteil vom 06.02.2013 entschieden, dass das Kind eines anonymen Samenspenders das Recht hat zu erfahren, wer sein biologischer Vater ist (Az. I-14 U 7/12). Es hat damit nicht nur dem Anliegen einer einzelnen jungen Frau Recht gegeben. Sarah P. wollte den Namen ihres biologischen Vaters erfahren und das OLG wertete das im Grundgesetz festgelegte Recht auf freie Entfaltung der Persönlichkeit höher als das Recht eines Spenders auf Anonymität. Die Klägerin hatte erst vier Jahre vor dem Urteil erfahren, dass ihre Mutter sich einst anonym hatte befruchten lassen. Weil sie ihren Vater kennenlernen wollte, verklagte sie den damals behandelnden Arzt auf die Herausgabe des Spendernamens. Vor dem Landgericht Essen hatte die 21-Jährige in erster Instanz keinen Erfolg. Eine Revision ließ das OLG nicht zu. Der Beklagte kann aber mit juristischen Kniffen beim Bundesgerichtshof (BGH) noch zu einem Revisionsgrund kommen.

Noch ist nicht klar, ob sie ihren Vater tatsächlich kennenlernen wird, weil sie die Bekanntgabe des Namens zwar notfalls in einem Zwangsvollstreckungsverfahren durchsetzen kann, der Arzt sich jedoch darauf beruft, die Daten zu dem Fall nicht mehr zu besitzen. Dem betroffenen Fortpflanzungsmediziner Thomas Katzorke droht ein Zwangsgeld oder Zwangshaft. Katzorke beruft sich darauf, dass die Unterlagen damals nur zehn Jahr aufbewahrt werden mussten. Das Urteil bezeichnete er als „rein theoretisch“. Tatsächlich wurde eine längere Aufbewahrungsfrist erst vorgeschrieben, nachdem die 21 Jahre alte Klägerin geboren war. Die Richter des OLG nahmen dem Mediziner seine Argumentation nicht ab. Bei einer Befragung hatte er sich in Widersprüche verstrickt und zugegeben, dass nicht alle Daten vernichtet wurden.

Das Urteil des OLG könnte nun eine Vielzahl ähnlicher Klagen nach sich ziehen. Sarah P. ist nicht die Einzige, die gerne ihren biologischen Vater kennenlernen würde. Etwa 100.000 Kinder sind seit den siebziger Jahren in Deutschland durch das Sperma von Samenspendern gezeugt worden. Im Moment gibt es in der Bundesrepublik etwa ein Dutzend Samenbanken. Anonyme Spenden sind heute nicht mehr erlaubt.

Vor ein paar Jahrzehnten entschieden Gerichte noch, es gehöre zur geschützten Intimsphäre der Frau, den Erzeuger ihres ledigen Kindes nicht nennen zu müssen. Dass Kinder das Recht auf Auskunft über den anonymen Samenspender erhalten, zeigt, dass im Familienrecht die Moral inzwischen der Wissenschaft weicht. Aus der Entwicklungspsychologie ist bekannt, wie wichtig das Wissen um die eigenen Wurzeln für die Ausbildung der Persönlichkeit ist. Neben Vater und Mutter hat sich inzwischen das Kind als zentraler Bezugspunkt des rechtlichen Schutzes in der Familie etabliert. Bereits 1989 hatte das Bundesverfassungsgericht entschieden, dass es zu den Persönlichkeitsrechten eines Menschen gehört, seine genetische Herkunft zu kennen. Auch die UN-Kinderrechtskonvention räumt allen Kindern dieses Recht ein. Für die Reproduktionsmedizin wurde 2007 eine Neuregelung erlassen. Gemäß dem seitdem geltenden Gewebegesetz müssen Unterlagen zu einer Samenspende 30 Jahre lang aufbewahrt werden.

Während der Umgang mit Daten bei Samenspenden in anderen europäischen Ländern klar geregelt ist, herrscht in Deutschland Verunsicherung. Die Kenntnis des Spendernamens ermöglicht Kindern die Geltendmachung von Unterhalts- und Erbschaftsansprüchen, die an der biologischen Abstammung anknüpfen. Der Leiter der Erlanger Samenbank Andreas Hammel forderte Konsequenzen aus dem Urteil. Der Gesetzgeber solle die Modalitäten des Auskunftsrechts regeln und Samenspender vor Unterhaltsforderungen schützen. Zudem sollten lesbische Paare, die in eingetragener Partnerschaft leben, heterosexuellen Eltern gleichgestellt werden. Die Dokumentation der Spenderdaten müsse möglichst auf eine staatlich finanzierte Einrichtung – ähnlich den Krebsregistern – übertragen werden (Janisch, Kliniken müssen Namen und Samenspendern nennen, Das „Ich“ zählt, SZ 07.02.2013, 1, 4; Tochter darf Namen von Samenspender erfahren, www.sueddeutsche.de 06.02.2013).

VG Leipzig

Jobcenter muss Diensttelefonliste offenlegen

Das Verwaltungsgericht (VG) Leipzig hat mit Urteil vom 10.01.2013 der Klage einer mit Sozialangelegenheiten befassten Anwaltskanzlei auf Zugang zur

Diensttelefonliste mit den Durchwahlnummern der mit Bürgerkontakt tätigen Mitarbeitenden des Jobcenters Leipzig stattgegeben (Az. 5 K 981/11).

Das Jobcenter Leipzig ist telefonisch für die BürgerInnen nur über eine zentrale Servicenummer erreichbar; die telefonische Durchwahl zur SachbearbeiterIn ist organisatorisch nicht vorgesehen. Diese Praxis besteht bundesweit. Wer eine Arbeitsagentur anruft, landet zunächst in einer Warteschleife, in der mitgeteilt wird: „Willkommen in Ihrer Agentur für Arbeit“. Die Anrufenden können die „2“ drücken, „wenn Sie Fragen rund um das Thema Arbeitslosengeld II haben, auch bekannt unter Hartz IV“. Beim Kindergeld gilt die „5“, bei allen anderen Angelegenheiten die „8“. Die Bundesagentur für Arbeit (BA) kanalisiert die telefonischen Anfragen bundesweit über einheitliche Hotline-Nummern, damit die Sachbearbeitenden in ihren Büros ungestört die Gespräche mit den Arbeitslosen führen können. Das vorliegende Urteil stellt diese Praxis nun in Frage.

Den Antrag der Anwaltskanzlei auf Zugang zur Diensttelefonliste mit den Durchwahlnummern der MitarbeiterInnen, den diese auf die Regelungen des Informationsfreiheitsgesetzes gestützt hatte, lehnte das Jobcenter ab. Nach erfolglosem Widerspruchsverfahren hat die Klage Erfolg. Das Informationsfreiheitsgesetz (IFG) sieht einen umfassenden Informationsanspruch zu amtlichen Informationen vor, soweit dagegen nicht Sicherheits- oder Datenschutzgründe sprechen. Sicherheitsgründe sah das VG Leipzig im vorliegenden Fall nicht. Die Diensttelefonnummern der Bearbeitenden einer Behörde unterliegen nach dem IFG nicht dem persönlichen Datenschutz des einzelnen Bediensteten. Die innere Organisation des Jobcenters allein sei kein Kriterium, das dem Informationsanspruch der BürgerIn entgegen gehalten werden kann.

Der in diesem Fall erfolgreiche Leipziger Rechtsanwalt Dirk Feiertag hält diese Entscheidung für überfällig. Eine schnelle Hilfe für Arbeitslose werde „durch die Abfertigung der Betroffenen in einem Callcenter systematisch verhindert“. Martin Künkler von der Koordinierungsstelle der gewerkschaftlichen Arbeitslosengruppen begrüßt den Richterspruch ebenso: „Es ist ein Ärgernis, dass es für Arbeitslose nicht möglich ist, ihren Vermittler direkt anzurufen, um bestimmte Probleme schnell zu klären.“ BA-Vorstandsmitglied Heinrich Alt twitterte dagegen, das Urteil sei „nicht praxistauglich“. Die Behörde weist darauf hin, dass die insgesamt 76 Callcenter für Arbeitslose und Hartz-IV-Empfänger jährlich gut 30 Millionen Anrufe erhielten. Mehr als 80% der Anfragen ließen sich sofort klären. Jeder Jobsuchende könne über die Hotline einen persönlichen Gesprächstermin mit seinem Vermittler buchen, der nur so Zeit und Ruhe hätte, mit dem Arbeitslosen zu reden. Das Jobcenter Leipzig will in Berufung gehen (PM VG Leipzig v. 10.01.2013; Öchsner, Auskunft unter dieser Nummer, www.sueddeutsche.de 22.01.2013).

VG Schleswig

Facebook sichert vorläufig seine Klarnamenpflicht

Das Verwaltungsgericht (VG) Schleswig hat mit Beschlüssen vom 14.02.2013 zwei Anträgen der Facebook Inc./USA und der Facebook Ireland Ltd. auf vorläufigen Rechtsschutz gegen Anordnungen des Unabhängigen Landeszentrums für Datenschutz (ULD) Schleswig-Holstein stattgegeben (Az. 8 B 60/12, 8 B 61/12). Damit stellte das Gericht die aufschiebende Wirkung der Widersprüche gegen die Verfügungen wieder her. Anlass für die Entscheidung des Gerichts ist die von Facebook angestrebte Klarnamenpflicht: Nutzende des Netzwerks sollen bei der Registrierung auch tatsächlich ihren echten Namen angeben und nicht irgendeinen erfundenen. Wer dies nicht so tut, muss damit rechnen, dass sein Konto gesperrt wird. Eine Freigabe soll nur dann erfolgen, wenn sich der Nutzende mit einem amtlichen Lichtbildausweis identifiziert.

Das ULD ging hiergegen vor und erließ zwei Verfügungen: Facebook sollte seinen NutzerInnen die grundsätzliche Wahlmöglichkeit darüber überlassen, bei der Registrierung auch Pseudonyme nutzen zu können. Außerdem sollte das Unternehmen alle bereits gesperrten Nutzerkonten wieder freigeben. Die Behörde ordnete die sofortige Vollziehung an und drohte ein Zwangsgeld an. Facebook legte gegen diese Bescheide Widerspruch ein und begehrte gleichzeitig vor dem VG die Wiederherstellung der aufschiebenden Wirkung. Das VG entsprach diesem Antrag. Nach Ansicht des VG Schleswig lassen sich die Verfügungen des ULD nicht auf deutsches Datenschutzrecht stützen, da Facebook keine Niederlassung in Deutschland habe sondern in Irland. Damit sei aber irisches Datenschutzrecht anwendbar.

Das VG führte aus: Bei der hier vorzunehmenden summarischen Prüfung erweise sich die Anordnung der Entsperrung der Konten als rechtswidrig. Das Datenschutzzentrum habe seine Anordnung zu Unrecht auf das deutsche Datenschutzrecht gestützt. Dieses sei jedoch nicht anwendbar. Nach der Europäischen Datenschutzrichtlinie und dem Bundesdatenschutzgesetz finde das deutsche Recht keine Anwendung, sofern die Erhebung und Verarbeitung von personenbezogenen Daten durch eine Niederlassung in einem anderen Mitgliedstaat der Europäischen Union stattfinde. Dies sei hier der Fall: Die Facebook Ireland Ltd. erfülle mit dem dort vorhandenen Personal und den dortigen Einrichtungen alle Voraussetzungen einer Niederlassung in diesem Sinne mit der Folge, dass ausschließlich irisches Datenschutzrecht Anwendung finde. Die Facebook Germany GmbH hingegen sei ausschließlich im Bereich der Anzeigenaquise und des Marketing tätig. Daher sei sowohl die Anordnung der Entsperrung als auch die Zwangsgeldandrohung rechtswidrig. Nicht relevant sei, dass die wesentlichen Inhaltsdaten in Deutschland nicht nur erhoben, sondern hier auch von dem Dienstleister Akamai gespeichert und verarbeitet werden.

Der Leiter des ULD Thilo Weichert kommentierte die Beschlüsse: „Die Entscheidungen sind mehr als verblüffend und gehen in der Argumentation über das Vorbringen von Facebook hinaus, das die Nichtanwendbarkeit des deutschen Datenschutzrechtes damit begründete, Facebook Inc. in den USA sei nur der Auftragsdatenverarbeiter der Facebook Ireland Ltd. Sie sind in sich

widersprüchlich, wenn sie die fehlende rechtliche Relevanz von Facebook Germany damit erklären, dass dort keine Daten verarbeitet würden, zugleich aber das Unternehmen in Irland für zuständig erklären, obwohl dort auch keine Daten verarbeitet werden. Die Beschlüsse hätten zur Folge, dass eine One-Stop-Shop-Regelung, wie sie in einer europäischen Datenschutz-Grundverordnung – kombiniert mit einem ausgeklügelten Kooperationssystem der Aufsichtsbehörden – geplant ist, für die IT-Unternehmen gar nicht nötig wäre. Es käme nur darauf an, die Konzernstruktur so zu gestalten, wie es Facebook tut, also eine Niederlassung in einem EU-Staat mit niedrigem Datenschutzniveau für zuständig zu erklären. Dies war nicht die Regelungsabsicht der Europäischen Union." Das ULD kündigte an, die Beschlüsse des VG Schleswig vor dem Schleswig-Holsteinischen Oberverwaltungsgericht mit Beschwerden anzufechten (Verwaltungsgericht gibt Eilanträgen von Facebook statt, www.schleswig-holstein.de/OVG/ 15.02.2013; VG Schleswig: Facebook mit Eilanträgen gegen ULD erfolgreich, www.telemedicus.info; Verwaltungsgericht Schleswig erteilt Facebook Freifahrtschein, www.datenschutzzentrum.de 15.02.2013).

AG Halle

Klage gegen Google wegen Beleidigung zurückgewiesen

Das Amtsgericht (AG) Halle hat am 08.01.2013 die Klage des Hallenser 42-jährigen Künstlers Tomas Alexander Hartmann gegen Google wegen des Vorwurfs der Beleidigung abgewiesen. Hintergrund ist ein Blog-Eintrag durch einen Unbekannten auf einer von Google betriebenen Webseite, auf der Hartmann als Psychopath beleidigt wurde. Der Kläger forderte Unterlassung und Entfernung der verleumderischen Behauptungen. Der Suchmaschinengigant hatte den Eintrag im Oktober 2012 vorerst löschen müssen, nachdem das Gericht eine einstweilige Verfügung aussprach. Diese wurde nun mit der Entscheidung aufgehoben.

Google selbst hatte inzwischen die verleumderischen Texte tatsächlich entfernt. Die Überschrift war aber über eine Suche noch zu finden, in bestimmten Angeboten sogar noch der gesamte Text. Der Kläger, der ohne Anwalt auftrat, hatte im Ergebnis keinen Erfolg. Zum einen sei für die von Google betriebene Plattform blogger.com, auf der besagte Beleidigung zu lesen war, Google in den USA zuständig. Anstatt das Unternehmen in den Vereinigten Staaten zu verklagen, richtete sich der Fokus Hartmanns auf die deutsche Google-Niederlassung in Hamburg. Zudem hatte der Kläger neben dem Amtsgericht in Halle auch das Amtsgericht in Hamburg eingeschaltet. Auch wenn er die dortige Klage wieder zurücknahm – die Amtsrichterin in Halle meinte, dass man nicht dieselbe Sache an verschiedenen Gerichten anhängig machen dürfe. Deshalb sei die Klage in Halle unzulässig.

Die Klage sei aber auch inhaltlich nicht begründet. Google Deutschland betreut hauptsächlich Geschäftsfelder wie etwa die Werbung. Suchmaschineneinträge oder Blogger-Dienste seien nicht Aufgabe der hiesigen Niederlassung. Google stellte einen entsprechenden Antrag und bekam Recht. Die Prozesskosten hatte der Kläger zu tragen; er hat die Möglichkeit, in Berufung zu gehen. Statt dies zu tun, kündigte der Kläger an, es mit einer Klage in den USA erneut probieren zu wollen (Amtsgericht Halle weist Klage wegen Rufmord auf Google-Webseiten ab, www.pc-magazin.de 08.01.2013; Gericht weist Beleidigungs-Klage gegen Google ab, www.focus.de 08.01.2013; Krämer, Verleumdungen Hallenser verklagt Google, www.mz-web.de 10.12.2012).

Buchbesprechung



Plath, Kai-Uwe (Hrsg.)
BDSG – Kommentar
Köln 2013, 2116 S.

tw Die Landschaft der gedruckten BDSG-Kommentare ist in letzter Zeit bunter geworden: Neben den Loseblattsammlungen Möhrle/Herb und Schaffland/Wiltfang und den „Oldies" Gola/Schomerus und Simitis sowie Däubler/Klebe/Wedde/Weichert kam 2010 Taeger/Gabel und nun aktuell der Plath auf den Markt. Die beiden letztgenannten Werke bearbeiten nicht nur das BDSG als Kernmaterie, sondern auch Datenschutzvorschriften im Telemediengesetz und im Telekommunikationsgesetz. Da diese Gesetze in der Praxis eine wichtige Rolle spielen, sind die Erläuterungen eine gute Hilfe, ohne dass gesondert weitere Werke angeschafft und konsultiert werden müssen.

Das deutsche Datenschutzrecht erweist sich als eine äußerst umfangreich und qualifiziert behandelte Rechtsmaterie. Der Wettbewerb zwischen den Kommentaren trägt zu deren Qualität bei. Was sie unterscheidet, ist eher die Ausrichtung und das adressierte Publikum, was stark durch die jeweiligen AutorInnen bestimmt wird. Der „Plath" ist ein Praktikerkommentar ohne einen expliziten wissenschaftlichen Anspruch, aber wohl mit dem Anspruch auf umfas-

sende Bearbeitung der aktuell relevanten juristischen Fragen. Diesem Anspruch wird er voll gerecht. Bearbeitet und dargestellt werden nicht nur die eigenen Positionen, sondern auch die aktuelle Rechtsprechung, das Schrifttum, inclusive anderer Meinungen, und Festlegungen von Aufsichtsbehörden. Dabei werden eher verarbeitungsfreundliche Positionen vertreten; diese werden aber regelmäßig qualifiziert begründet. Dies gilt z. B., wenn Kamlah meint, neben dem § 28a BDSG sei noch Raum für Datenverarbeitungen auf der Grundlage von Einwilligungen, wenn Plath meint, Unterauftragsverhältnisse müssten in einem Auftragsvertrag nur generell vorgesehen sein, um zulässig zu sein, oder wenn Plath/Schreiber meinen, bei der Frage der wirksamen Anonymisierung personenbezogener Daten sei auf die subjektive Sicht der verantwortlichen Stellen abzustellen.

Eine erfreuliche Tendenz wird auch vom „Plath" verfolgt: Während bei einigen der Oldies die Bereitschaft zur Behandlung aktueller neuer technischer Themen zunächst gering war, ist die Themenbreite hier von Anfang an auf dem Stand der Zeit. Social Media, Cloud Computing, Scoring, Online-Targeting sind inhaltlich also keine Fremdworte. Ein Defizit aller juristischen Kommentare liegt aber auch hier vor: die eher reduzierte rechtliche Behandlung technischer Sachverhalte.

Andrea Hauser, Ina Haag
Datenschutz im Krankenhaus
4. Auflage
Deutsche Krankenhaus Verlagsgesellschaft mbH, Düsseldorf, 2012
ISBN 978-3-942734-25-7
EUR 45,00

ks Die datenschutzkonforme Gestaltung von Abläufen im Krankenhaus verlangt von Verantwortlichen regelmäßig die Analyse und Bewertung komplexer Sachverhalte und juristischer Normen. Angefangen bei der korrekten Gestaltung des Behandlungsvertrages über den Fluss der Patientendaten im Krankenhaus bis zur Archivierung sind sehr viele und sehr unterschiedliche Prozesse rechtskonform, patientenfreundlich und gleichermaßen praktikabel zu gestalten.

Die beiden Autorinnen geben im vorliegenden Buch einen sehr umfangreichen und gut strukturierten Überblick über datenschutzrechtliche Fragestellungen des Klinikbetriebs.

Sie verwenden zunächst viel Sorgfalt auf die detaillierte Darstellung gesetzlicher Grundlagen und das Verhältnis von Datenschutz und ärztlicher Schweigepflicht. Die folgenden zentralen Kapitel widmen sie dem Umgang mit Patientendaten – und zwar sowohl innerhalb des Krankenhauses als auch in Fällen, die eine Übermittlung an Stellen außerhalb erfordern. Diese Kapitel sind anhand zahlreicher Beispiele und Bezüge auf aktuelle Rechtsprechung sehr anschaulich gestaltet und daher für die Praxis hilfreich.

Es folgt ein leider sehr dünn geratenes Kapitel zum datenschutzgerechten Umgang mit Mitarbeiterdaten, in dem die Problematik der allgegenwärtigen Leistungs- und Verhaltensdaten in modernen Krankenhausinformationssystemen leider vollkommen unerwähnt bleiben.

Die anschließenden Kapitel greifen erneut Aspekte der Übermittlung von Patientendaten an externe Stellen auf – allerdings unter dem Gesichtspunkt gesetzlicher Vorgaben zu Abrechnungs- und Kontrollprozessen. Hier finden sich systematische Darstellungen der Rahmenbedingungen zur Übermittlung an Sozialversicherungsträger, Krankenkassen, Unfallversicherungsträger u.a.

Die folgenden Betrachtungen zu Dokumentation und Archivierung im Krankenhaus können lediglich als Orientierung dienen. Zu diesem zugegebenermaßen schwierigen Themenkomplex gibt es bessere und fundiertere Veröffentlichungen. Ein Blick in die Literaturliste offenbart, dass die Standardveröffentlichungen, gerade auch in Zusammenhang mit elektronischen Patientenakten, nicht zur Kenntnis genommen wurden.

In diesem Zusammenhang wird das Hauptmanko des Buches besonders deutlich: die informationstechnischen Aspekte wurden fast vollständig ausgeblendet.

Zu viele Aspekte, die in heutigen informationstechnisch durchorganisierten Kliniken besonderer datenschutzkonformer Gestaltung bedürfen, bleiben leider unerwähnt: der Rundum-Einsatz von Krankenhausinformationssystemen, die Schnittstellen zu externen Systemen (z. B. Laborinformationssystemen), der zentrale Aspekt der Gestaltung von Berechtigungssystemen, die Gestaltung von und der Umgang mit elektronischer Pflegedokumentation, das Erfordernis technischer und organisatorischer Schutzmaßnahmen, wie z.B. Verschlüsselung (gerade in Zusammenhang mit Archivierung), die Anforderungen an Online-Befundübermittlung, um nur einige zu nennen.

Dass an einer der wenigen Stellen, an denen konkret auf technische Maßnahmen Bezug genommen wird (Entsorgung) eine veraltete DIN statt der aktuellen DIN 66399 zitiert wird, scheint ein symptomatischer Schönheitsfehler.

Das eingangs sehr einprägsam dargestellte gesetzlich begründete „Zwei-Schranken-Prinzip" wird zum Erstaunen des Lesers bei der Darstellung der Auftragsdatenverarbeitung (ADV), z.B. durch EDV-Dienstleister nicht mehr thematisiert. Es wird vielmehr der falsche Eindruck erweckt, dass das Vorliegen eines ADV-Vertrags mit einem Dienstleister den Patienentendatentransfer legitimiert. Dass dies nur die datenschutzrechtliche Seite betrifft, eine Datenverarbeitung im Auftrag jedoch keine Offenbarungsbefugnis im Sinne des § 203 StGB schafft, bleibt unerwähnt.

Das Kapitel über den Datenschutzbeauftragten beschränkt sich leider auf die Reproduktion und Erläuterung der entsprechenden Vorgaben des Bundesdatenschutzgesetzes. Was fehlt, ist die praxisorientierte Darstellung, wie ein Krankenhaus-Datenschutzbeauftragter in der schwierigen Gemengelage sinnvoll agieren kann. Hier hätte man sich Anregungen und Vorgaben für ein systematisches Datenschutzmanagement erhofft – und insbesondere die Aussage, dass es ohne ein solches nicht geht!

Es wäre zu wünschen, dass die Autorinnen in einer hoffentlich folgenden, weiteren Auflage ihres sehr übersichtlich und systematisch aufgebauten Buches die informationstechnischen Aspekte des Themenkomplexes stärker berücksichtigen würden und den Index zu einer praxisbezogenen Arbeitshilfe ausbauen würden. Als systematisches Übersichtswerk ist das Werk dennoch bereits jetzt zu empfehlen.

Videoüberwachung:

Hat man sich erst an die stationären Kameras gewöhnt, werden danach unauffällige INDECT-Drohnen die Revolution in der Verfolgbarkeit von Individuen einleiten.

Ihre Gedankenpolizei.

